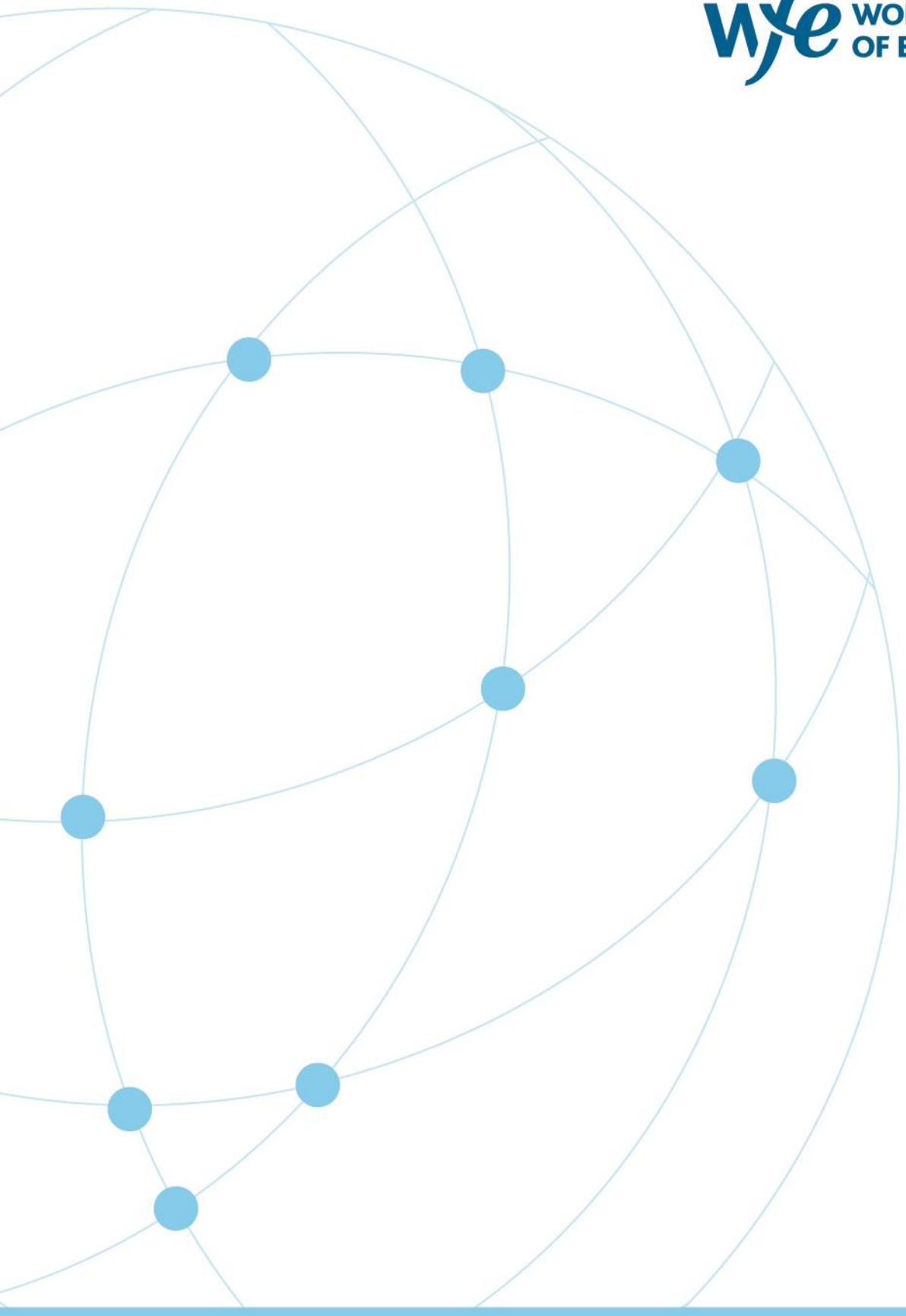

Response: FSB Consultative Document – Achieving Greater Convergence in Cyber Incident Reporting

31st December 2022

Background

The World Federation of Exchanges (WFE) is the global trade association for regulated exchanges and clearing houses. We represent the operators of over 250 market infrastructures, spread across the Asia-Pacific region (37%), EMEA (43%) and the Americas (20%), with everything from local entities in emerging markets to international groups based in major financial centres. In total, member exchanges trade around $100 trillion a year and are home to some 60,000 companies, with an aggregate market capitalisation of around $120 trillion. The 50 distinct central counterparty (CCP) clearing services (both vertically integrated and stand-alone) collectively ensure that traders put up $1 trillion of resources to back their risk positions.

With extensive experience of developing and enforcing high standards of conduct, WFE members support an orderly, secure, fair, and transparent environment for all sorts of investors and companies wishing to invest, raise capital and manage financial risk.

Founded in 1961, the WFE seeks outcomes that maximise financial stability, consumer confidence and economic growth. We also engage with policy makers and regulators in an open, collaborative way, reflecting the central, public role that exchanges and CCPs play in an internationally integrated financial system.

If you have any further questions, or wish to follow-up on our contribution, the WFE remains at your disposal. Please contact:

Chhavi Sinha, Regulatory Affairs Manager: csinha@world-exchanges.org

Richard Metcalfe, Head of Regulatory Affairs: rmetcalfe@world-exchanges.org

Nandini Sukumar, Chief Executive Officer: nsukumar@world-exchanges.org

Response:

The WFE welcomes the opportunity to comment on the consultative document published by Financial Stability Board (FSB) on Achieving Greater Convergence in Cyber Incident Reporting, which sets out recommendations to address impediments to achieving convergence, advances work on establishing common terminologies related to cyber incidents and proposes the development of a common format for incident reporting exchange (FIRE).

WFE welcomes FSB's efforts regarding broader convergence in Cyber Incident Reporting (CIR). Recently, WFE members have noted that multiple incident reporting requirements of different authorities/regulators are creating problems in respective jurisdictions, and it will be good to explore how these requirements can be harmonised. Members have expressed views that it will be difficult to have a standardised template as a standardised template would not work in those situations where different variable and people are involved. In view of the same, the WFE has developed a guide for its members that provides for the applicable content that is helpful to include in cyber incident reporting. The guide is expected to allow individual organisations to craft templates that make sense within their own organisation, based on risk appetite and on their local regulators' requirements.

Considering the above initiative, the WFE supports FSB's concept of FIRE that authorities could further develop and eventually use to collect incident information from Financial Institutions (FIs) and for authorities to use for information sharing. We believe that FIRE would provide flexibility to allow a range of adoption choices and include the most relevant data elements for financial authorities.

We have responded to selected questions from the consultation paper below.

Specific Comments

Section 2: Challenges to achieving greater convergence in CIR

Questions

1. Is the emphasis on practical issues to collecting and using cyber incident information consistent with your experience? Does your institution want to provide any additional evidence for the FSB to consider from your experience?

   Answer: Yes, the WFE's experience has been consistent with some of the practical issues in using/collecting cyber incident information as identified by FSB in Section 2. We agree with the FSB's finding that meaningful differences in how different authorities determine their reporting criteria for cyber incidents, use incident information and set their timeframes for reporting an incident pose operational challenges for FIs; particularly for FIs that operate across many jurisdictions and sectors and are subject to multiple reporting requirements for one incident, with each notification tending to trigger follow-up enquiries from each financial

authority. In addition, many FIs are required to notify law enforcement, cyber insurance, industry threat sharing groups, customers, and stakeholders within set timeframes, as well as internally, to business continuity teams, corporate executives, and corporate communication teams.

The WFE members have reported that multiple incident reporting requirements of different authorities/regulators are creating problems in respective jurisdictions. Particularly, in terms of critical infrastructure, incident reporting is to be made and to two different audiences: a) Sectoral level— the body in charge of the financial sector; b) National level—where there is a cyber security agency that looks after all the critical infrastructure. In terms of the content reported to each of these parties, challenges are faced because from a financial sector view, they tend to want to look at the financial markets impact, whereas, from a cyber security agency perspective, they tend to want to look at how you protect the nation. So, when a request for information is made, there is tendency of overlapping information, because each agency has a different collecting method (and the templates that they use tend to be different). The WFE members have felt that some form of co-ordination among the different agencies, in terms of providing information in a more consistent manner, would help to relieve some of these problems that are faced by the organisations.

The WFE members have reported that if an organisation sits globally, its reporting requirement demand increases, for example, a member (that operates globally) may be required to report under Swiss Financial Market Supervisory Authority (FINMA), Digital Operational Resilience Act (DORA) [EU] and other national guidelines. The different authorities have different standards, making it difficult to meet their demands.

Similarly, there are several legislations, for example, within the US regarding reporting of cyber security incidents and there is considerable redundancy across the different regulators around the globe. Each jurisdiction or each regulator may have some sort of templates that the FIs have to comply with when reporting to the regulators.

Section 3: Recommendations

Questions

Are there other recommendations that could help promote greater convergence in CIR?

Answer: The WFE supports most of the recommendations listed in Section 3. Particularly, the WFE believes that to promote convergence among CIR frameworks, a clear incident reporting objectives and impact of an incident must be defined within a FI. It is also important to define what constitutes an incident whether it includes targeted and malicious incident. Within that targeted concept, some filtering criteria as to what should be reported within the materiality element can be decided. In this regard, the WFE supports Recommendation 8 which requires financial authorities that use materiality thresholds to explore adjusting threshold language,

or use other equivalent approaches, to encourage FIs to report incidents where reporting criteria have yet to be met but are likely to be breached.

It is also important to provide for a better information sharing mechanism and operational mechanism between authorities. In this regard, the WFE supports Recommendation 11 that provides for financial authorities to explore methods for collaboratively addressing legal or confidentiality challenges relating to the exchange of CIR information on a cross-border basis—including using Memorandum of Understanding (MoUs), or other equivalent arrangements, to outline the basis for the information exchange between authorities, which typically include commitments to maintain the confidentiality of information. We also support Recommendation 12 that requires financial authorities to engage regularly with FIs to raise awareness of the value and importance of incident reporting, understand possible challenges faced by FIs and identify approaches to overcome them when warranted.

Section 5: **Format for incident reporting exchange (FIRE)**

Questions

1. Would the FIRE concept, if developed and sufficiently adapted, usefully contribute towards greater convergence in incident reporting?

   Answer: The WFE Members have expressed views that it will be difficult to have a standardised template for Cyber Incident Reporting as a standardised template would not work in those situations where different variables and people from IT, legal, Communications and HR are involved. In view of the same, the WFE has developed a guide for its members that provides for the applicable content that is helpful to include in cyber incident reporting. The guide is expected to allow individual organisations to craft templates that make sense within their own organisation, based on risk appetite and on their local regulators' requirements. As per the WFE guide, the essential data fields to be considered in incident reporting includes: 1. **Determining the relevant authorities and regulatory framework**; 2. **Reporting Timeline** (whether the reporting should be made within 24 hours to 72 hours of an incident) ;3. **Definitions** (how the key terms such as **incidents** and **materiality** are defined within the relevant Regulations), 4. **Scope of Reporting** (this should cover significant incidents as defined by the relevant rules of the concerned jurisdiction); 5. **Reporting Mechanism** (how and to whom the reporting and disclosures should be provided); 6. **Impact Assessment** (the evaluation and articulation of impact for incident reporting purposes) ; and 7. **Incident Closure report.**

   Considering the above initiative, the WFE supports FSB's concept of FIRE that authorities could further develop and eventually use to collect incident information from FIs and for authorities to use for information sharing. We believe that FIRE would provide flexibility to allow a range of adoption choices and include the most relevant data elements for financial authorities. Such a format, if further developed, would not require strict global convergence and could be flexible to consider co-existence. Authorities can decide the extent to which they wish to adopt FIRE, if at all, based on their individual circumstances.

   The WFE, however, encourages the FSB to collaborate with similar initiatives around the globe to avoid fragmentation. In the past, the WFE has held a stand that it is important that any

proposed framework is compatible (as far as possible), or can be implemented, globally and by all sectors in the ecosystem. Such an approach would also help to avoid inadvertent fragmentation and conflicting regulatory requirements in different jurisdictions, ensuring that the proposals are informed by, and aligned to important international guidance. A harmonised and coherent approach is particularly relevant for future initiatives. Conflicting practices may result in regulated entities needing to implement multiple sets of requirements, adding to the risk of confusion and inefficient implementation.[1]

[1] WFE Response to the Bank of England/PRA/FCA Operational Resilience Consultations, October 2020