Consultation Response

UK Incident Reporting & Outsourcing Registers: PRA CP 17/24 & FCA CP 24/28

March 2025

AFME welcomes the opportunity to respond to the joint FCA/PRA consultation papers on UK Incident Reporting & Outsourcing Registers (PRA CP 17/24 & FCA CP 24/28).

AFME represents a broad array of European and global participants in the wholesale financial markets. Its members comprise pan-EU and global banks as well as key regional banks, brokers, law firms, investors, and other financial market participants. We advocate stable, competitive, sustainable European financial markets that support economic growth and benefit society.

We are responding from the perspective of our bank members and have focused on those issues which are most relevant to wholesale capital markets. Given the level of interest in this consultation we have responded to each of the questions within the FCA consultation materials and we remain available to discuss any of the specific answers in further detail.

In addition to our responses below on each of the posed questions, we raise these three broader points:

1. **We would strongly encourage the authorities to be more ambitious in ensuring a cohesively joint approach:** While we recognise the authorities have different remits and statutory duties, we have identified many divergences between the PRA and FCA which undermine the benefits of standardisation which both authorities are rightly seeking to secure as part of these proposals. This is illustrated in the templates, in the secondary factors for consideration on incident reporting and in terms of when notifications on material third parties should be submitted. We would urge the authorities in each of these cases to adopt uniformity and have indicated which of the proposed provisions are seen to be more effective. We would stress that the current misalignment, for example over how to determine if a third party arrangement is material, will result in significant operational burden for firms as they conduct dual assessments, even if ultimately the authorities regard the net impact of the divergence as limited.

2. **The UK authorities have missed an opportunity to rationalise the wider set of disparate reporting regimes currently in place and to embed recent supervisory initiatives on operational resilience:** Financial institutions will now be faced with multiple UK incident reporting regimes, under PSD2, FCA Principle 11, PRA Rule 7, and potentially under cross sectoral frameworks on critical infrastructure operators, with significant impact on the UK competitiveness. Such duplication represents a significant operational burden for firms and only detracts resources from incident management, with no net benefit in terms of risk management. While other jurisdictions are working to minimise duplicate reporting, for example in the EU with DORA, it is regrettable the UK has not sought to do likewise. The proposals were also an opportunity to embed the UK's recently established Important Business Services (IBS) into incident reporting, and we would urge the authorities to rethink a direct link for those firms which have

IBS, notwithstanding the fact the scope of the proposals apply to some firms which do not have IBS.

3. **We welcome the intention to apply materiality but would urge authorities to go further and more explicitly lock in these safeguards:** By limiting the reporting of outsourcing arrangements to material third parties we acknowledge authorities are trying to ensure proportionality within the incoming Outsourcing Registers. Yet this is currently lacking with regards to incident reporting, where the low bar set by the operational incident definition will result in almost all incidents having to be triaged by firms, despite the operational burden. The definition should reflect the higher parameters outlined in the PRA and FCA thresholds. Materiality could also be embedded through a tightening of the draft wording, with authorities avoiding subjective criteria such as "may pose an impact" or capturing indirect impact. Other supervisory tools are on hand to identify interdependencies in the sector.

Consultation Questions

Question 1: Do you have any comments on the cost benefit analysis including our assumptions, assessment of costs and benefits to firms, consumers, the market and third parties?

- The financial sector disagrees with the cost benefit analysis (CBA). The FCA and PRA state that new 'standardised incident reporting' provides a benefit to incident management and that there are no additional costs incurred due to existing reporting processes being in place. The regulators are proposing an entirely new and highly prescriptive incident reporting framework, including detailed requirements for both the assessment of whether incidents are reportable, and specific data fields and taxonomies which need to be implemented. The detailed nature of the incident assessment criteria will necessitate the implementation of systems and processes for data collection; assessment; and evidencing of assessment outcomes. While the data requirements are broadly aligned to existing practice, it is unlikely that many firms will have all of these data elements included in their existing systems, much less likely that all of the proposed taxonomies and data definitions will already be in place. For many firms these processes leverage global systems. As such, systems change to implement these requirements is likely to be a significant cost by itself.
- An example of these sorts of costs includes the experience of any bank with regards to the recent implementation of DORA, where the uplifts resulted in a significant cost (by way of illustrating the scale at stake, one member estimated a €2.3m CtB cost and €3.8m RtB cost). The increased cost is in part driven by the costs in triaging incidents to determine whether each is reportable, and this not being reflected in the volume of actual submitted reports. We estimate that for every submitted report a firm will have triaged roughly 40 potentially reportable incidents. This equates to approximately 90 hours of triaging non-reportable incidents since 17th January's go-live application, and for one significant credit institution bank entailed including sending out 46 assessments for completion by ops teams. This illustrates the important of thresholds which are suitably clear and high level so that firms are able to minimise the number of incidents they need to consider triaging for possible DORA reporting.

- As the proposal does not repeal PSD2 reporting or replace informal operational incident reporting that occurs via Fundamental Rule 7 and Principle 11[1], or a variety of cyber and related incident reporting, the financial sector disagrees that the new regime would result in no additional costs and believes the disparate reporting regimes would result in greater cost, higher burden and an increased complexity in doing business in the UK. Developing a separate incident reporting process for the FCA and PRA in this proposal will result in an additional cost and administrative requirement that would entail further staffing and governance requirements being placed into firm's incident management processes. This would be far in excess of the identified £1.5k implementation cost within the consultation materials, likely by several orders of magnitude at a minimum, and would be exacerbated by our view that the authorities have failed to realise the volume of reporting which will materialise under the incoming regime, from the very low thresholds being proposed. Higher implementation costs would be mirrored by higher running costs, given the incoming three stages of reporting. Again by way of comparison, the recent Target 2 outage resulted in one bank spending approximately 50 hours in completing all three stages of EU DORA reporting, including having to send out 48 different assessments for completion by various Ops teams.
- The financial sector believes that the lack of recognition of the burden of PSD2 reporting alongside two separate FCA and PRA criteria in the CBA is a material gap. The UK would have the widest variety of reporting regimes being applicable to financial services of any equivalent jurisdiction. The Financial Stability Board's (FSB) Format for Incident Reporting Exchange (FIRE) initial report into convergence of cyber incident reporting regimes states that authorities should seek convergence, adopt common data requirements and calibrate reporting windows[2]. The financial sector supports the repeal of PSD2 reporting, via a statutory instrument or waiver/modification, and further clarity provided on the expectations around 'operational incidents' that are not reportable under the new proposals, but may be reportable under Principle 11 and Fundamental Rule 7. To deliver this, AFME members would encourage the regulators to defer their proposals for an incident reporting framework until such a time as they have the legislative basis on which to incorporate PSD2 reporting, and to allow them sufficient time to conduct a comprehensive review of existing reporting requirements, to enable the development of a coherent and efficient reporting framework.
- The CBA states that firms will benefit from the proposal as there will be greater clarity concerning the information that is required in an incident notification. Members therefore wish to clarify that authorities will not request additional information outside the reporting phase timelines and stated data fields unless there is a material risk for not doing so. Members have experienced material requests for further granular information when reporting in the UK, which are often requested inconsistently across similar incidents. As this information is different from the data fields included in the proposal, the sector is unclear to what extent the stated benefit will be realised. In this respect, we would encourage PRA/FCA supervisory teams to be engaged by regulatory policy colleagues as part of the development of these proposals to ensure that the proposed notification data attributes accurately reflect the incident reporting process that firms will face. Conversations to date with officials have raised concern that the PRA and FCA are not fully aligned in terms of whether *ad hoc* communications with supervisory teams during an incident would be superseded by the incoming regime, or sit in parallel to it.

[1] Note that, per the CBA within the FCA response, certain firms can have supervisory agreements to report operational incidents per Principle 11 and Fundamental Rule 7 in specific formats. The financial sector is not suggesting the repeal of Principle 11 and Fundamental Rules 7 and acknowledges their role within supervisory practices.

[2] https://www.fsb.org/2023/04/recommendations-to-achieve-greater-convergence-in-cyber-incident-reporting-final-report/

- Both the FCA and PRA state that a benefit to firms is the ability for each respective regulator to work with firms to 'prepare for emerging risks,' to 'use data gathered to enable future work' and 'monitor market-wide risks'. These all indicate that the reporting regime is being utilised for data collection purposes and not to improve incident remediation or management capabilities of individual firms. While members welcome the verbal assurances that information from the initial and intermediate reports should not be used for these broader purposes, we would stress neither is the final report the most appropriate tool for such analysis. There are multiple other bodies and public-private sector interactions (e.g. CMORG, FS-ISAC, firm supervision) whereby authorities have the capability to request data and prepare and discuss market-wide risks with firms. An incident reporting regime that is predicated on data collection-only for authorities conflates incident management and diverts firm attention from remediation to information collection.
- In seeking to develop a one-size-fits-all incident reporting framework, the regulators have eschewed the use of components of the operational resilience framework which have been implemented by in-scope firms. This has introduced significant duplication of effort for those firms, while introducing additional ambiguity both for the incident reporting requirements and for the already implemented operational resilience requirements. Members would strongly endorse the introduction of two separate regimes, one for those firms in scope of operational resilience requirements, and one for those which are not. The regime applicable to in-scope firms would then be able to leverage the significant work already undertaken by setting thresholds for reporting at the level of a firms being likely to imminently breach its IToL. This would achieve the regulators' stated goals while removing significant ambiguity, operational burden and likely over-reporting.
- Members believe that a harmonised incident reporting regime, per the initial recommendations of the FSB, could result in benefits to firms. A more considered proposal across the FCA and PRA, which reduces duplications, seeks convergence and adds clarity could aid the competitiveness of the UK. Examples of benefits include:
    - The FCA and PRA should further base the incident reporting regime on the existing operational resilience regime applicable in the UK. This would help embed the relatively new IBS and Impact Tolerances (IToLs). All considerations for IBS and IToLs reflect the secondary thresholds of the PRA and FCA and members reject the hypothesis of the PRA/FCA that a non-IBS operational incident can affect financial stability (PRA) or cause intolerable harm (FCA)[3]. The decision within the EU to align the DORA incident reporting framework with a firm's Critical and Important Functions (CIFs) was a welcome alignment which greatly assisted implementation and ensured proportionality. If an operational incident effects the availability of service for a non-IBS, the internal classification of that incident should be the basis of any other reporting or the ethos of Principle 11 and Fundamental Rule 7 should apply.
    - A repeal of PSD2 incident reporting requirements via a statutory instrument repealing 'The Payment Services Regulations 2017, SI 2017/752, Part 7, Regulation 99' subject to the implementation of the proposed rules. Additionally, the FCA has the capability to provide firms with waivers or modifications which allow non-compliance with specific rules. Members therefore support a statutory instrument, that could be introduced via a Financial Services Bill, being put into effect before the implementation deadline or a waiver to PSD2 reporting for all payment service providers operating in the UK. This would result in the single

[3] The PRA defines Important Business Services as "the services a firm provides which, if disrupted, could pose a risk to the firm's safety and soundness or the financial stability of the UK" and the FCA defines IBS as "services which, if disrupted, could potentially cause intolerable harm to the consumers of the firm's services or risk to market integrity." These definitions directly align to the reporting thresholds stated by each regulator.

reporting approach in the UK, which would reflect how NIS reporting has been successfully harmonised in the EU under DORA.
  - Confirmation that a single reporting format is acceptable for all 'operational incident' reports and that only one report would be required for both regulators for dual-regulated firms.
  - Confirmation by the FCA and PRA that any additional Requests For Information (RFI) relating to each incident should be aligned to the timelines included in each proposal. All RFIs should have practicable timelines and request consistent information.

Question 2: Do you agree with the proposed definition of an operational incident?

- The definition is regarded as overly broad in scope, to the extent it would essentially capture any incident, including potentially planned events such as systems upgrades. Even with the application of higher thresholds as part of a firm's assessment of an incident, this would result in an overly burdensome approach to incident reporting. This is further complicated if firms are anticipated to triage all incidents to confirm whether they constitute an 'operational incident' before triaging each incident according to each assessment criteria included in the FCA and PRAs proposals (which are conflicting in scale). This triaging would need to be documented and evidenced by firms in anticipation of future supervisory review, creating a direct cost associated with every incident that falls within this definition, regardless of its materiality.
- In particular, we have significant concern that the definition as proposed contains no materiality lens. AFME would strongly recommend this is inserted into the definition:
  - An ***unplanned*** single event or a series of linked events that ***materially*** disrupts the firm's operations, where it either:
    - disrupts the delivery to the firm's clients or a user external to the firm of:
      - ***an important business service for those regulated firms which are within scope of the Operational Resilience framework (SS1/21); or***
      - ***a critical and essential service for those firms outside the UK Operational Resilience framework (SS1/21)***
    - impacts the availability, authenticity, integrity or confidentiality of information or data relating or belonging to the firm's clients or a user external to the firm"
- Additionally, the regulators use slightly different wording for their definitions with no apparent reason or benefit. We would strongly encourage the regulators to use a single consistent definition across both regulations to promote consistency and avoid unnecessary complexity and confusion.
- It is unclear what the regulators mean by "end user external to the firm", and the differentiation of this term versus more established and well-understood terminology such as "client" or "consumer". We would encourage the regulators to make use of more established terminology to avoid unnecessary confusion, inconsistency and complexity in the regulatory environment.
- The extension of the definition to include impacts on data and information is itself an enormous scope of incidents. This would require every single misdelivered email to be formally assessed against the criteria, regardless of the materiality, reviewed, subjected to governance, recorded and possibly reported to the regulators. This would introduce a significant operational burden, redirecting resources away from critical incident management, and likely make it difficult for the regulators to delineate the important incidents. We would also note that in comparison, under DORA, data loss is a single factor out of several required for the assessment of whether an incident should be reportable,

and in this case considers the criticality of the data rather than seeking to make all data impacts reportable.

- Members would additionally seek clarification that the second sub-clause does not imply firms are required to ascertain the impact on data held externally by clients or third party providers. Such information sits outside the firm's line of sight and should be captured by the incoming reporting requirements as part of the UK critical third party (CTP) regime.

Question 3: Do you agree with the thresholds for firms to apply when considering reporting an operational incident to us? Are there other factors firms should consider when reporting operational incidents?

- As proposed, there is a significant disconnect between the overly broad definition of an operational incident, the higher parameters of the thresholds (which we support), and the very low nature of the outlined factors for consideration. A simplified proposal, that would equally recognise the current UK regime and ensure proportional reporting figures, would base the regime on existing IBS that have been identified by each regulated firm, or equivalent for those firms who are not within scope of the IBS framework.
- The reporting thresholds of the PRA and FCA align directly to the definitions provided by the PRA and FCA for IBS in their respective operational resilience regimes. Members support this and believe that, as the operational resilience regime has been effectively embedded within firms and the UK financial sector, the reporting thresholds and the disruptions to IBS should be the basis of the incident reporting regime even if the terminology cannot be directly replicated to all firms in scope of the incident reporting obligations. This could explicitly be referenced by the authorities stating that the thresholds, for firms in scope of Operational Resilience requirements, be summarised as: "Firms must submit an operational incident report in the event that, due to an incident, they are likely to breach one or more Impact Tolerances".
- Moreover, the purpose of this exercise should not be to set new requirements for how firms identify important business services and set their impact tolerances or to review how firms have done so. Any concerns with how an individual firm has set their IBS should be addressed through other supervisory tools and engagements. If the regulators wish to prompt a broader review of impact tolerance levels, then this should be communicated clearly and separately.
- Incidents that do not relate to IBS or the UK's resilience regime could still be captured by a firm's internal classification criteria, and subject to the continued application of Principle 11 and Fundamental Rule 7, thereby ensuring that supervisors remain informed concerning the incidents that could affect the PRA and FCA's mandates. Furthermore, both the PRA and FCA have the capability to produce guidance and inform firms if they are not reporting effectively or according to levels they require. This could be considered after the introduction of a more proportionate regime.
- Members strongly oppose the inclusion of subjective criteria within incident reporting regimes. Incident management should not be diverted to subjective analysis that speculates on 'potential' impact, 'operational and financial contagion'[4] or 'may pose a risk'. Reporting regimes should be grounded in objective facts and data about a realised operational incident. Members strongly welcome the verbal assurances from the authorities that there is no intention to capture "near-misses" in the incoming framework,

[4] Should the authorities be seeking to leverage and extend the use of the term operational contagion, we would strongly encourage explicit engagement with industry in advance. The term has been included within a Financial Policy Committee paper and has since been included in three rulesets for Critical Third Parties, Financial Market Infrastructures and now incident reporting. This has been without industry consultation despite the high complexity and subjectivity involved in determining how 'operational and financial contagion' can be quantified or reflected by an individual financial institution.

and would recommend the removal of the above phrases/terminologies to give effect to these assurances. The concern is that otherwise firms will have to err on side of caution and adopt an approach which lacks proportionality and materiality as demonstrated in the FCA Case Studies 1, 3 and 5. The suggestion that each of these would be sufficient to trigger reporting is causing high level of concern given that: case study 1 indicates no threshold in terms of the number of clients impacted; case study 3 indicates no actual harm has yet arisen or is imminently going to occur; and case study 5 fails to recognise that consumers were diverted and access reinstated, thereby indicating this issue is one of inconvenience rather than intolerable harm. With regards specifically to the FCA threshold on Consumer Harm, this causes particular concern in that it would include incidents which "*could cause*" harm, and AFME proposes that the authorities tighten their approach by replacing in this instance "could cause" with the phrase "*likely to imminently cause*". We urge the same revision with regards to the wording in the draft PRA SS 2.13, which currently reads "could result" in significant disruption to the service.

- Similarly, we urge the authorities to remove references to indirect harm. While we understand that authorities are seeking to understand inter-dependencies within the market, we doubt that incident reports would serve as the most effective tool for regulators to map interconnectedness. The incoming CTP regime will provide one alternative, without causing delays in incident reporting by forcing firms to reach out and explore how Nth parties may have been impacted. This is illustrated within the FCA Case Study 4, where there is no value in having Firm G report on the indirect impact, given that Firms E and F would have already reported the incident, and there is a lack of practicality in requesting firms to gauge the potential impact inside another entity. This lack of practicality is also reflected in Case Study 7 which implies firms are required to gauge whether and when clients are comfortable and prepared to reconnect. In addition to the delays, and bearing in mind our previous points explaining that these assessments will need to be conducted for an extremely large number of incidents, attempting to assess indirect impacts for every incident will represent an enormous operational burden and cost on firms for little or no benefit, and likely to the detriment of firms' incident management capabilities. Additionally, given that in many cases firms will not be able to determine the scale of indirect impacts to any degree of certainty, they may be required to over-report to a significant degree to avoid the risk of supervisory sanction for under-reporting.
- Additionally, there are factors for consideration which are inappropriate for the purposes of incident management in that they are not relevant for the purposes of assessing, triaging and providing actionable support to firms while they are responding to an incident, for example the factors relating to a firm's legal and regulatory omissions or its reputation. Firms would be naturally hesitant to provide information which may imply a legal or regulatory failing, and including such factors for consideration would only counteract the spirit of openness and transparency which we understand UK authorities are seeking to build upon. Including such considerations will therefore hinder the authorities in boosting reporting by viewing it as constructive engagement. In practice, minor contractual breaches can often be dealt with bilaterally between the parties involved with little or no impact on firms' safety and soundness, market stability or customer harm. It is unclear how, in the vast majority of cases, a breach of regulatory or legal obligations is likely to meet these thresholds. The FCA Case Study 6 also illustrates well the unintended consequences of this criteria, in that it is likely the scenario may amount to a breach of wider employee rights legislation and yet, it is rightly regarded as a non-reportable incident. Members encourage that the FCA/PRA consider the removal of this criteria as was equally removed from the final reporting requirements for DORA.
- Consequently, we are concerned with two of the outlined purposes of incident reporting:
    - *get a better understanding of the operational resilience of individual firms and the financial services sector more broadly*

- *identify potential vulnerabilities and areas for improvement.*

This is shifting the underlying rationale of incident reporting away from actionable intelligence, and towards broader data collection. We would stress that there are other tools for authorities to gather general information and insights, for example the BoE's joint industry forums including the FSCCC, the Sector Response Framework groups such as CMORG. Incident reporting should continue to be clearly framed and understood as part of incident management and response. Regulatory rulemaking and enforcement should be undertaken by supervision and not via an incident reporting regime. Additional haphazard references to other regulatory regimes, for example the referral to the ICO within the FCA Case Study 10 should be avoided, at least without greater clarity as to the level of joint supervisory expectations.

- With regards to the FCA case studies, while we welcome the efforts of the authorities to provide industry with additional clarification and guidance, we question the currently proposed set of 10 case studies. The current level of specification appears to conflict with a firm's responsibility to set its own impact tolerance levels or alternatively contain little value in focusing on clear cut examples of non-reporting, for example as with case study 2. Instead we would suggest the FCA focus on 3 case studies which demonstrate clearly the level of materiality which the authorities regard as the tipping point for reporting. And in drafting these case studies would encourage the FCA to be explicitly mindful of wider, existing operational resilience measures, for example whether an IBS or equivalent has been breached, and also the cumulative impact on competitiveness from excessive overreporting of information which is not actionable. We propose the following three case studies and would be happy to discuss these further:
  - **Case study 1: the need for materiality within UK reporting:** Firms A and B are UK-based banks undergoing a merger. During the merger, there is a failure in the integration of IT systems. This results in clients losing access to their accounts and being unable to process transactions; a service which both banks have identified as an Important Business Service. The banks communicated with affected clients but were unable to provide an alternative route for them to access their accounts in order to execute transactions within the firms' stated impact tolerance levels. The disruption to service has caused intolerable harm, and so the firm correctly considers that a report is due.
  - **Case Study 2: why incidents causing indirect impact on the firm's clients and wider sector should <u>not</u> be captured:** Firm E provides clearing services to Firm F, who in turn provides trade execution services for Firm G, a consumer investment firm. Firm E suffers an outage at its data centres, which means it cannot receive orders for clearing trades or ensure that orders are reconciled. As Firm F relies on Firm E for clearing, this disruption means Firm F could not execute trades. The disruption at Firm F leads to a failure to serve Firm G, and prevents clients from trading through Firm G. Each firm should report with regards to the direct impact on its services and clients. Firm E will not have sight of the indirect impact on Firm G and so should not be expected to delay reporting while it tries to ascertain this information. Even with indirect impact removed from scope, authorities will have received 3 separate reports on the same underlying incident.
  - **Case study 3: Incidents harming the firm's reputation:** Firm K is a UK bank that offers retail banking services. An Information Technology-focused news publication that publishes stories concerning cybersecurity incidents publishes a story about Firm K being subject to a significant cyber-attack. The story is false and all of Firm K's Important Business Services are operating without any reduction in their availability. As there is no impact to customers, Firm K does not

report the incident formally through the FCA Portal. The news story, however, could affect the firm's reputation and be of relevance to notify the FCA about. Firm K informs the FCA regarding the news story and lack of impact through their requirements to inform the regulator of relevant information under Fundamental Rule 7.

- The criteria for reputational impact is also a concern due to the examples, including Case Study 8, having limited interaction with the secondary thresholds. The PRA, for instance, requires reports on the basis of financial stability or a firm's safety and soundness, but requests reputational incident reports for incidents with social media or local news coverage.

Question 4: Do you agree with the proposed approach to standardise the formats of incident reporting?

- The goal of standardisation is warmly welcomed and supported by AFME. We stress though it is currently undermined by the level of divergence between the FCA and PRA in their outlined approaches, definitions and factors for consideration. While we understand each authority must separately update their own regulatory guidance (Handbook/Rulebook/Supervisory Statements) the failure to adhere more ambitiously to joint definitions and approaches is a missed opportunity to embed standardisation.
- Any benefit accrued due to the standardised formatting is negated by the continued application of PSD2. PSD2 requires multiple intermediate reports, which could be concurrently applied during another report being submitted on the basis of the new FCA and PRA proposals. One member experienced a PSD2 reportable incident with a maximum of 15 intermediate reports and other members regularly experience 3-4 intermediates with relative frequency. The volume of PSD2 reports also fails to capture the full operational burden to banks, who will have to triage many potentially reportable incidents, a substantial share of which will then not meet the required thresholds. Members noted that while PSD2 reporting figures are not necessarily high, this does not account for the triaging of the incident to determine reportability, the continued use of a separate incident classification and the FTE required. One member submitted approximately 25 reports but triaged 70, constituting a far higher level of burden than the reporting figures would imply. An equivalent payments incident would still require triaging on the basis of PSD2, FCA, PRA, FR7 and PRIN11 even if the incident is not reported. A metrics-based payments incident reporting regime, with alternative formatting, fields and timelines, being applicable alongside two alternate FCA and PRA assessment criteria is an unnecessary reporting burden which increases the cost and complexity of doing business in the UK vis-à-vis other jurisdictions.
- With regards specifically to the stages and formats of incident reporting, we would suggest this is facilitated by joint wording in terms of determining when initial, intermediate and final reports become due, and in particular shared use of the proposed FCA terminology on initial reports, namely that these are due "*as soon as it is practical to do so".*
- In addition, we note that a number of fields are repeated across initial, intermediate and final report templates. It would be helpful if these datapoints could be carried over by the authorities, and only require update where there is a change.
- Further, while we would have supported in principle the proposal to shift the intermediate reports away from time-based determinants, and for these to be triggered on the basis of a 'significant change' in the incident, the possibility of multiple intermediate reports becoming due has negated any perceived benefits in this change of approach. Instead we have concluded the UK should continue to align with other

jurisdictions in seeking *one* intermediate report 72 hours after the initial report was submitted, or as soon after as it is practical to do.

- Should the UK authorities adhere to their proposed approach, we would strongly urge both to adopt the same definition of "*significant change*" and to embed materiality safeguards. While the two proposed sets of definition may not appear to amount to significant divergence, the variations in wording causes confusion and exacerbates the operational burden on firms. Joint definitions would also protect against any revision by one of the authorities not being replicated by the other authority.
    - A more simple criteria that an intermediate report is required once i) an incident materially affects one further assessment criteria, ii) has increased in severity according to a firm's internal classification of the incident or iii) has affected another IBS, would be sufficient.
    - Any incident which is ongoing for any period of time will have a constantly increasing severity of impact. With the current drafting, firms would in effect have to submit a new intermediate report every day during an extended incident as the impacts were updated. This would be an enormous undertaking, and divert significant resources away from the actual management of the incident, with little benefit. New information will frequently come to light at various points throughout the management of the incident, much of which will not be material in and of itself. Submitting an intermediate report every time a new detail becomes available would be extremely onerous and costly, impacting the UK's competitiveness, with limited benefit.
    - To this end, we in particular would urge the authorities to remove the following from the two definitions of substantial change, on the basis that such a step is in practice a minor development in incident management or a determinant for the final report:
        - *When the firm has taken action to mitigate the impact of the incident.*
        - *Whether the firm has deployed a business continuity plan.*
        - *When the incident is resolved.*
        - *The activation of a business continuity plan, disaster recovery plan or significant changes to the resolution strategy of the operational incident.*
        - *The firm resolving the operational incident.*
        - *The impact of an operational incident becoming more severe.*
        - *The operational incident breaching another regulator's reporting threshold for submitting an operational incident report after the submission of the initial report to the PRA.*
        - *When additional information is available that provides more context on the incident.*
        - *When the known impact of an operational incident changes.*
- Regarding the Final report, the FCA propose that, where incidents originate in a third party, firms "take reasonable steps" to get information about the root cause of the incident from the third party. In practice this will not always be possible, as in some circumstances there may be security or legal reasons that the third party is unable to disclose the information. Instead, we would propose that this be amended to require firms to "make reasonable enquiries".
- The mutually sought benefits of standardisation are additionally undermined by the expectation of the PRA for separate notifications by firms, in addition to the reports submitted through the incoming online platform. This has created confusion and we would recommend that informal alerts to authorities are dealt with separately outside the scope of this proposed incident reporting framework.
- Further, to unlock the benefits of standardisation on a global basis, we would strongly encourage the authorities to more closely adopt the FSB FIRE template as the format for

UK incident reporting. A 'standardised template' for each jurisdiction presents little value for industry, especially firms operating across multiple global locations. There remain a number of inconsistencies in terminology and wording between the FSB and the PRA/FCA formats where it is unclear regarding the benefit to the wording differences or why they have been adapted. An additional gap analysis across all data fields should be considered, with the UK starting with full alignment and with deliberate justifications for amendments.

- Cumulatively, the above duplication, in terms of overlapping reporting frameworks, the possibility of a misaligned FCA/PRA approach, and the prospect of multiple intermediate reports, results in a situation which substantively undermines the relative competitiveness of the UK as a jurisdiction.

Question 5: Do you agree that we are being proportionate and is collecting the right information at the right time to meet its objectives? Is there other information that should also be collected for a better understanding of the operational incident?

- The initial incident report is required at a critical time during the management of an incident, and should be kept to the minimal possible fields required for the regulators' purposes at that point in time. Each data element should be carefully assessed to determine whether it is absolutely necessary, and where it is not, it should be deferred to later reports. As a starting point, members have proposed that the following fields be deferred to the intermediate report:
    - Incident discovery method
    - Estimated time to resolve the incident
    - Actions planned to recover
    - Actions taken to recover
    - Public reaction to the incident
    - Public communication issued
    - Other regulatory bodies notified
    - Type of the business service affected
    - Time of the occurrence (if known)
    - Time of the detection
    - Time of the resolution
    - Level of geographic spread
    - If multi-jurisdictional, list the geographic codes
    - Indicative root cause
    - Incident origin
- There are some fields for which members would propose amendments:
    - Estimated time to resolve the incident – In many cases it is not possible to estimate the time required to resolve an incident, and while we recognise that this is optional, should firms be unable to complete it, removal would avoid the potential for questions being raised which may distract from the management of the incident.
    - Public reaction to the incident – It would be helpful for the regulators to specify that this should only be completed when incidents are over a certain threshold, as minor incidents are not likely to attract public attention.
    - What proportion of an impact tolerance has been used – We would be interested to understand more what the regulators' use of this data field would be. There is a risk that it would ultimately be used through supervision to introduce a cumulative ITOL, which is something that has been determined to not be desirable through industry consultation and engagement on the operational resilience framework.

  - Notification of contractual/regulatory breaches – As discussed in our comments on the criteria for assessment of whether the threshold has been breached, we would propose these be removed. Contractual breaches should be dealt with on a bilateral basis, and will only require escalation in exceptional circumstances, and the reporting of regulatory obligation breaches is already covered in the majority of regulations themselves, and does not here account for the materiality of either the breach or the regulation.
- AFME welcomes the broad alignment with the FSB FIRE format. We note though the misalignment over Resource Type, where we would stress that such divergences require significant manual remediations.
- Finally, we would again stress that members are concerned that any benefit from the removal of an enforced intermediate reporting phase would be negated when multiple intermediate reports would be required each time a significant change criteria is met. An FCA report requiring multiple intermediates once new 'additional information is available' could result in an indiscriminate number of intermediate reports that will be disproportionately burdensome and likely result in the UK required the highest number of incident reports of any equivalent jurisdiction.

Question 6: Do you agree with the proposed definition of third party arrangements?

- We appreciate the PRA and FCA's efforts to streamline reporting requirements and to align definitions and approaches under their respective frameworks. To that end, we welcome the aligned definition of third-party arrangements. Acknowledging the need for some divergence in approach given the regulators respective mandates and objectives, we believe there is an opportunity to further enhance these efficiencies and the alignment of approaches throughout the proposed Outsourcing and Third Party (OATP) reporting framework ('OATP framework'). Such harmonisation would help reduce complexity for firms operating across both frameworks and help give effect to the regulators' shared objectives to develop a streamlined and interoperable framework.
- We encourage the authorities when finalising the draft definitions and thresholds, to more explicitly consider the link to the authorities' use of the information being sought via the registers. The operational burden to firms from adapting and maintaining the registers is significant, and so we would strongly encourage that any uplift be justified with a gain in terms of resilience and risk management. The anticipated operational uplift is currently considered to be high, given that the registers will deviate from existing approaches and templates, and therefore require significant manual remediation to establish and put in place.
- With regards to intragroup providers, it is also our understanding that this is what is being referred to under the third component of the proposed definition (*provided by a person within the same group of the firm*). We would suggest that the term *entity* instead of *person* would be clearer and should therefore be used.
- The definition also refers to "*An arrangement of any form between a firm and service provider*". It would be clearer to clarify this is an arrangement by which a service provider provides a service to the firm, and therefore does not include for example a business referral.
- Additionally, we propose refining the scope to products and services provided "*on a recurrent or ongoing basis*" in line with the FSB Toolkit and DORA.
- Relatedly, the definition of subcontractors could be further aligned with a risk-based approach by revising the scope to subcontractors 'whose disruption will *materially* impair the continuity of the firm's *material third-party* service'. This recognises that not every subcontractor linked to a material third-party service would have the same level of importance or potential impact to the provision of the service.

Question 7: Do you agree with the proposed definition of material third party arrangements?

- AFME welcomes the regulators' commitment to a risk-based and proportionate approach and the application of a materiality threshold to the scope of third-party arrangements. This targeted approach ensures an appropriate balance between oversight and operational efficiency to support effective risk management.
- However, we note that the proposed use of "*pose a risk to*" is inherently broad and lacks a materiality threshold. Given the expanded scope of the proposed OATP framework, the distinction between the terms "*pose a risk to*" and "*materially impair*" carries certain implications for firms' risk assessment and reporting processes. It risks capturing an overly broad scope resulting in overreporting and a divergence from the regulators' intended objective to capture those arrangements that could have a tangible impact, rather than merely a theoretical potential for harm. By contrast, the term "*materially impair*" emphasises actual, significant impacts. We therefore suggest the regulators replace "*pose a risk to*" with "*materially impair*" in their respective definitions of 'material third-party arrangement'. This amendment should be reflected across the regulators' policies (i.e. paragraphs 5.5, 5.11, 5.11A., 5.20 and 5.20A of Draft SS2121).
- It is critical though that materiality is thoroughly embedded in the UK's framework, through its application within the outlined factors for consideration when determining a third party as material. Further, while we understand the need for separate definitions on Material Third Parties within the FCA Handbook and PRA Rulebook, we do not agree with the lack of synchronisation on the FCA factors for consideration/PRA materiality criteria. Even if the divergence in criteria may not be significant, the misalignment creates additional complexity for firms' risk management without benefit to risk management and supervisory expectations.
- We appreciate the regulators' taking a risk-based approach to intragroup arrangements and distinguishing these from external third-party arrangements. Whilst acknowledging that strong oversight is needed for intragroup arrangements, forcing a single framework for both external and internal outsourcing fails to recognise differences in risks and operations. Members also welcome the verbal assurances from the authorities that intragroup providers should not be seen as material unless supported by third parties. However, we would encourage further guidance from the regulators as to the appropriate treatment of intragroup arrangements and how these should be reported, specifically noting the PRA's guidance that intragroup arrangements without an external provider would not necessarily be considered material.

Question 8: Do you have any comments on our proposed notification requirements including the impact on the number of arrangements that will be reported?

- We note that the regulators have diverged in their approaches to the proposed notification requirements and we would again encourage alignment. The PRA requires notification of '*material third-party arrangements which, due to the associated risks, necessitates a high degree of due diligence, risk management or governance by the firm*'. The FCA requires notification of '*all material third-party arrangements*' without further specification. This divergence risks creating inconsistencies in implementation and reporting. While we appreciate the PRA's efforts to provide further specificity and clarity, and perhaps a more focused scope of material third-party arrangements to be reported, the PRA's approach ultimately adds further complexity without benefit to risk management practices or a risk-based approach. In this case, firms would welcome the

PRA aligning with and adopting the FCA's simpler framework. This would also seem to align with the approach taken by the PRA in complementary policies.

- In addition, we consider the introduction of additional criteria and guidance as to when the regulators expect a material third-party to be notified introduces unnecessary complexity, that may in fact undermine the regulator's objective of ensuring consistency in materiality assessments. This is illustrated in the PRA's examples of arrangements which should not trigger notification being at odds with the FCA, in the absence of an exclusion for functions which are statutorily required. We propose the regulators simplify this process and simply require notification of third-party arrangements that firms determine are material based on the definition and materiality assessment criteria. This would help mitigate the anticipated uplift in volume of notifications expected to be reported once the new regime comes into effect.
- We also seek clarification as to the expectations of the authorities on the intended approach to the notification template. We acknowledge the regulators' intention to simplify the reporting burden for entities by merging the notification and register templates. We also note the regulator's acknowledgement that full completion of the entire template at the notification stage may not be operationally feasible and is not necessarily expected. However, rather than updating the template iteratively, it would be more efficient to complete certain data fields at notification and subsequently update the template at the annual register submission. Given this, we recommend that the following data fields, which may not be available at the notification stage, be made optional for initial submission:
    - Contract start/service start date (ID 3.06 and 3.07): As notification occurs before service commencement, these dates will not be finalised at the point of notification and requiring them could result in firms providing indicative rather than confirmed timelines. The service start date is likely to prove particularly challenging given that the service start date will depend on the notification period having concluded. It is much more likely that the contract execution date will be known, however this is not certain especially when contracting out of the UK.
    - Date and outcome of audit (ID 6.05 and 6.06): We note that the PRA has asked for both (i) date and outcome of most recent risk assessment, as well as (ii) most recent audit, i.e. distinguishing between both as separate activities. Whilst it would be typical for entities to undertake a risk assessment at onboarding, it would be less likely that entities would be undertaking an audit (despite being contractually entitled to).
    - Function Information (ID 3.15, 3.16 and 3.17): The assessment of whether the arrangement supports an IBS is typically something which is undertaken on a look-back basis, often long after contract execution.
- We note that the PRA has proposed to exclude third-country branches from the material third-party register proposals. We support this but would encourage a parallel exemption from notifications, otherwise the use of the shared template means financial entities will regardless have to collect all the data points.
- Under the amendments to SS2/21 we additionally note firms are expected to notify regulators upon occurrence of a change to a contract with a material third party. It is worth noting that some major suppliers may not have committed to specific timeframes for supporting such notifications. If the PRA requires a notification upon occurrence, then there may a need for requirements to be placed directly on suppliers.
- Finally, we welcome the proposal that notifications be made "*in a timely manner*" which further embeds a proportionate approach within the OATP framework.

Question 9: Do you think the mechanism to submit and update the structured register of firms' material third party arrangements is proportionate?

- Having noted that the authorities intend to set-up an FCA online portal/platform for the annual submission of the register, we assume this information will be shared with the PRA, and would therefore question why notifications should not be submitted through the platform for similar onward sharing. AFME is highly aware of the operational burden to firms from maintaining these third party mechanisms, and would encourage the authorities to adopt a streamlined approach where possible.
- We would also encourage the authorities to engage further with industry and would be supportive of a Dry-Run exercise on a best efforts basis. Such an exercise could help to identify a number of unforeseen issues and provide firms and authorities the opportunity to test the technical feasibility of the register against the data quality expectations of officials and provide any additional feedback. This would be particularly helpful in the event that alignment between the FCA and PRA as proposed in this response does not come to fruition.

Question 10: Do you have any comment on the template which includes the information on third party arrangements to be shared with us?

- AFME welcomes in principle the standardised approach, via inclusion of a template, as an effective means by which to ensure proportionality, but would note this is currently undermined by the level of divergence between the PRA and FCA. Given that multiple jurisdictions are likewise adopting third party registers, the level of international divergence is inevitably going to grow (as seen for example with the EU DORA Register of Information, which is limited to only ICT arrangements). It is critical therefore that authorities within the same jurisdiction have a joined-up and consistent approach.
- In particular we note the following points of divergence:
    - Whilst the overall number of datapoints in the PRA and FCA template align, the templates themselves do not align. In particular, we note that:
        - The PRA template has 6 tabs whilst the FCA's has 7 tabs.
        - The data fields in Tab 7 in the FCA template are part of another tab in the PRA template.
        - Reference numbers do not align for 25 datapoints.
        - Certain datapoints have slightly different names.
        - The PRA has not adopted the FCA taxonomy on Substitutability.
    - In the Outsourcing Register templates and supporting materials, we urge the PRA to mirror the exemption within SUP 16.33.6 for *"functions that are statutorily required to be performed by a service provider where the FCA already receives the related information (for example, through a statutory audit)."*
    - The industry assumption had been that firms would submit once to the RegData Platform for both the PRA and FCA. Given the differences in the templates (noted below), standardisation is required to ensure that firms do not need to populate two templates with the same information to be uploaded twice.
- Additionally, we provide the following feedback on specific aspects or data fields within the template. (Note: although the ID references relate to the PRA template, the feedback should also be taken to apply to the corresponding data fields in the FCA template):
    - **ID 2.05** - FRN of the firm receiving the service appears unnecessary in addition to an LEI.
    - **ID3.06 –** Requires date of contract commencement and service commencement; burdensome and unnecessary, the service commencement date is not always known at the time of contract commencement date and may vary depending on location etc.

- **ID 3.07** – Date of service commencement seems to be a duplication to Date of contract commencement
- **ID 3.08** - Notice period for the service provider – It is unclear what use this data field would be for the regulators. We would support the removal of this field.
- **ID 3.10** – Description of changes made to the contract is unnecessary; these will be reflected in the template as the details of the engagement are updated. Recommend this data field is deleted.
- **ID 3.11** – Description of changes made to the contract is unnecessary; these will be reflected in the template as the details of the engagement are updated. Recommend this data field is deleted.
- **ID 3.12 -** Next contract renewal date or end date – See above comments re: renewal.
- **ID 3.20-3.24 –** Data fields requiring information on impact tolerance are broken out (diverges from DORA approach; TBC whether feasible to provide this information.
- **ID 3.27** – The usefulness of this field for third party management/an industry level view for the regulators is not clear.
- **ID 4.03 –** LEI is required for TP but guidance to enter N/A if you cannot find TP in the look up tab is unclear; further clarity may be required.
- **LEI:** We do not consider the requirement to provide an LEI when identifying an alternative supplier is necessary or proportionate. For instance, whilst we may know the supplier we may not know the particular entity at this stage.
- **Type of Service/Service Category:** The terminology used here (i.e. use of "service" for both taxonomies) creates some confusion. We understand 'Service Category' to be a legacy taxonomy from the previous template, however it may be helpful to revise this to "Function Category" to distinguish it from the "Type of Service" taxonomy and reflect its relation to the business or corporate function (i.e. the IBS category).
- **Contract/Arrangement Ref Number:** The 'contract reference number' (a key relational field) is required in the second template (**ID 3.01**) but it appears there is no unique identifier that connects the various tabs of the templates. This might be addressed in the final templates, however we flag that the contractual reference number should be added to every tab (except for the first two tabs). Related to this, the template also calls for an 'arrangement reference number' (**ID 3.02**). This should not be necessary given that entities will now be providing a contract reference number (which is aligned with DORA register) and should be deleted.
- **Subcontractors:** Whilst it is not explicitly mentioned, we assume that only Tabs 4 and 5 are required to report subcontractor details (this should be clarified if not the case).
- **ID 6.03 / 6.08 / 6.10** – The FCA drop-down options (satisfactory; non-satisfactory; not done) should be applied to the PRA template.
- **ID 6.06** - Outcome of the most recent audit should include option of "not done" for on-going audits (at the point of reporting), where outcome is not completed/ not known.
- **Country of Jurisdiction:** It was suggested this could be added to the template.

- AFME is also conscious of how the UK proposals are diverging from the EBA Outsourcing Register templates with which firms are widely familiar. We would flag:
  - **Supply Chain Ranking:** We note that the requirement to 'rank' the subcontracting chain does not add value to risk management or supervision. It

does not reflect or have any relevance to how firms manage supply chain risk, which is to identify and manage the risks associated with 'material' subcontractors irrespective of their position in the subcontracting chain. It is also operationally challenging if not infeasible for firms to provide a ranking for all subcontractors across the supply chain. These concerns were highlighted through advocacy in connection with DORA and we urge regulators to deviate from the DORA approach in this regard. If, however, the UK regulators are to maintain this requirement, we encourage alignment with the methodology applied in DORA with respect to intragroup providers. Applying a rank 0 for intragroup providers also overlooks the reality of intragroup subcontracting chains. In such cases, it is unclear how firms would be expected to rank intragroup subcontractors (i.e. on the current approach all intragroup subcontractors would be 0 until the first external provider which may be further along the chain).

- We finally note that the excel based format is particularly cumbersome for amending or adding information, and leads to a potentially unlimited growth of tabs and rows. Other jurisdictions are moving away from excel in part for this reason, and we would request further engagement on this going forward. Given that the inclusion of Material Non-Outsourcing will greatly increase the submission size for larger firms, with one firm noting that the 2024 submission resulted in 400k rows of data, this represents a significant operational challenge. Moving to a relational template should have a positive impact, and future evolutions and updates to the templates should be clearly signposted with opportunity for industry input in advance. Given the overlap with the Supervisory Statement on Critical Third Parties to the UK Financial Sector, where the information submitted will be used for identifying and regulating the CTPs, it would be helpful to understand what efforts are being made to reduce duplicate reporting.