The City of London Law Society

4 College Hill
London EC4R 2RB

Tel +44 (0)20 7329 2173
Fax +44 (0)20 7329 2190
DX 98936 – Cheapside 2

mail@citysolicitors.org.uk

www.citysolicitors.org.uk

18 March 2025

By email: CP17_24@bankofengland.co.uk and cp24-28@fca.org.uk

Dear Sir / Madam,

PRA (CP17/24) and FCA (CP24/28): Consultations on operational incident and third party management reporting dated 13 December 2024 (the "Consultations")

1. The City of London Law Society ("**CLLS**") represents approximately 17,000 City lawyers through individual and corporate membership, including some of the largest international law firms in the world. These law firms advise a variety of clients from multinational companies and financial institutions to Government departments, often in relation to complex, multi-jurisdictional legal issues. The CLLS responds to a variety of consultations on issues of importance to its members through its specialist committees.

2. This response has been prepared by the CLLS Regulatory Law Committee (the "**Committee**" or "**we**"), a list of whose members can be found on the CLLS website. The Committee not only responds to consultations but also proactively raises concerns where it becomes aware of issues which it considers to be of importance in a regulatory context.

3. The Committee has considered the Consultations for additional requirements in relation to operational incidents and third party arrangements ("**TPA**"). We welcome the opportunity to present our views on the proposals.

4. Most of our comments are either common to both regulators' proposals or concern differences among the proposals. We therefore thought it may be more helpful to combine our comments together rather than dividing them into the individual consultations.

5. Our comments do not cover the Bank of England's parallel consultation in relation to requirements for financial market infrastructures (FMIs).

GENERAL COMMENTS

6. We have the following general comments across the consultations:

    a. Proportionality and adequate time for implementation will be important. Whilst recognising the stated policy objectives and practical benefits from enhanced firm reporting these areas, we expect that some of the new requirements, may be particularly onerous for smaller firms - for example, in relation to incident reporting, FCA firms which are not currently within the SYSC operational resilience regime or DORA (nor part of wider groups implementing DORA standards across their group). Sufficient time fo implementation will be required.

    b. Clarity and consistency between the new and existing requirements and definitions is critical. We note that generally the proposals would be additional to, and not amend or remove, existing reporting obligations; with several extra. but similar, definitions added on top of existing ones. The rule book taxonomy in relation to outsourcing and other third party arrangements is already layered. In certain areas (identified below), there is a risk that this multiplicity of requirements could give rise to uncertainty and/or unnecessary additional compliance. We encourage the regulators to consider carefully how the new requirements and definitions sit with existing rulebooks; and streamline where possible.

INCIDENT REPORTING

7. ***Definition of "operational incident":***

This is defined (using the FCA CP definition) as –

"either a single event or a series of linked events which disrupts the firm's operations such that it:

(a) disrupts the delivery of a service to the firm's client or a user external to the firm; or
(b) impacts the availability, authenticity, integrity or confidentiality of information or data relating or belonging to the firm's client or a user external to the firm."

Two elements of the definition are unclear and would benefit from clarification for firms:

- Firstly, what is meant by "disruption". Including whether this would include, for example, an event which happens at a third party service provider which does not actually impair a firm's ability to continue service delivery because of available back-up arrangements. Examples would be useful.
- Secondly, what is meant by "external user" (as distinct from a "client"). Examples would be useful.

8. ***Alignment with existing operational resilience requirements*:**

Currently, firms which are subject to the FCA/PRA operational resilience regime are required to identify resources which support their important business services and set risk appetite-based impact tolerances for potential disruption; and internal (and external) reporting thresholds will typically be aligned with those parameters. The PRA's proposals take into account these internal categorisation of operational incidents; the FCA's do not. We suggest that the FCA follows the same approach as the PRA, so that incident reporting decisions are aligned to a firm's business and risk model and that dual regulated firms do not need to carry out two assessments.

9. ***Level of reporting required:***

The proposals require three staged reporting in all incidents, even where there has been no impact on the firm's operations or its customers. In the interests of proportionality, we suggest that in such cases only an initial report (and maybe a second reporting to confirm no impact) would be sufficient.

10. ***Deciding whether to report – assessing the firm's ability to meet its legal obligations:***

Under proposed new SUP 15.14.9(4)G, the FCA expects firms to consider (when deciding whether to report) the firm's ability to meet its legal (and regulatory) obligations. This may not be feasible in the early stages of an incident. Firms should not have to speculate on such matters. A similar obligation was deleted from DORA's final version after consultation.

11. ***Payment services institutions - parallel obligations under PSR:***

We note that FCA authorised payment services institutions would be in-scope of the FCA requirements and also continue to have differently calibrated incident reporting obligations under the PSR (regulation 99(2) (Incident reporting)). FCA CP 24/28 states that the FCA does not expect all PSR notifications will meet the thresholds for reporting incidents under the new proposals; therefore there may be instances where payments firms will be required to report an incident under both regimes. We would encourage the FCA to try to find a unified notification arrangement to avoid duplication or even inconsistent reporting contrary to the FCA's objectives.

THIRD PARTY ARRANGEMENTS REPORTING

12. ***Inconsistency with existing requirements:***

The following are examples where we see potential confusion between the new requirements and definitions and the existing regime:

a. *Multiplication of similar but different definitions:* the proposals adds definitions, "third party arrangement" and "material third party arrangements", on top of existing similar existing definitions which are already uncertain and require subjective judgment - including "material outsourcing" or a "critical or important" function. "Material third party arrangement" in the FCA proposals is defined as:

"*a third party arrangement which is of such importance that a disruption or failure in the performance of the product or service provided to the firm could:*

(a) cause intolerable levels of harm to the firm's clients;
(b) pose a risk to the soundness, stability, resilience, confidence or integrity of the UK financial system; or
(c) cast serious doubt on the firm's ability to satisfy the threshold conditions, or meet its obligations under the Principles, or under SYSC 15A (Operational resilience)."

The definition in the PRA proposals is similar, but uses risks linked to the PRA's statutory objectives instead of the FCA's.

These definitions are materially wider than the existing definition of "material outsourcing". The existing FCA Glossary definition is limited to risks to the continuing satisfaction of the threshold conditions or compliance with FCA Principles. The PRA version is similar. This means that firms would need to consider two very different tests. Given that under the proposals an outsourcing is a sub-set of a "third party arrangement", this means two different assessments for a material outsourcing. There is no obvious logic for that. We recommend that the two definitions – and the list of factors which firms are expected to take into account in determining materiality - are fully aligned.

b. *Overlapping requirements for material outsourcings:* we note that the existing requirements to notify the FCA before entering into or significant changing a material outsourcing (under Principle 11 and SUP 15.3.8G) would remain but in-scope firms would be directed (under proposed SUP 15.3.10R) to report under the new reporting obligation for material TPA's. This approach seems unnecessarily complicated. A simpler approach would be disapply the existing obligation for in-scope firms - in line with the PRA's approach for its *PRA Notifications Rules 2.3(1)).* If the current FCA approach is retained, the guidance at proposed SUP 15.3.0G could be clearer.

13. ***Different reporting thresholds between PRA and FCA:***

The proposed PRA reporting threshold (requiring notifications only on a material TPA which, due to the risks, "necessitates a high degree of due diligence, risk management or governance by the firm) is narrower than the FCA and Bank of England proposals (which would require notification for all material TPA's). The rationale for this divergence is not entirely clear from the consultations. An aligned approach would better support the regulators' objective of more consistent reporting. The PRA's narrower threshold would mean that there could be a material outsourcing TPA which is not notifiable and a material non-outsourcing TPA which is notifiable.

14. ***Scope of "Third Party Arrangement" - services provided by another firm:***

It is unclear whether and if so in what circumstances a regulated entity providing services (whether regulated or not) to another regulated entity would be a 'service provider'. This is particularly important where the services are a mixture of regulated financial services (such as broking) and other (such as data supply). We recommend that this is clarified through the drafting of the rules or guidance, as the EU regulators have done in relation to ICT services providers under DORA (with

guidance to the effect that a regulated entity would qualify as a 'service provider' for DORA purposes only when providing standalone ICT services, whilst the provision of financial services that have an ICT component would not fall within the scope of DORA).

We hope the above feedback will be useful to you. If you would like to discuss any of these comments then we would be happy to do so. Please contact Hannah Meakin by telephone on +44 (0)20 7444 2102 or by email at hannah.meakin@nortonrosefulbright.com in the first instance.

Yours faithfully

Hannah Meakin
Chair, CLLS Regulatory Law Committee

© CITY OF LONDON LAW SOCIETY 2025
All rights reserved. This paper has been prepared as part of a consultation process.
Its contents should not be taken as legal advice in relation to a particular situation or transaction.