TheCityUK

TheCityUK response to FCA CP24/28 and PRA CP17/24: Operational Incident and Third-Party Reporting

Introduction

TheCityUK is the industry-led body representing UK-based financial and related professional services. We champion and support the success of the ecosystem, and thereby our members, promoting policies in the UK and internationally that drive competitiveness, support job creation and enable long-term economic growth. The industry contributes 12% of the UK's total economic output and employs over 2.4 million people – with two thirds of these jobs outside London across the country's regions and nations. It pays more corporation tax than any other sector and is the largest net exporting industry. The industry plays an important role in enabling the transition to net zero and driving economic growth across the wider economy through its provision of capital, investment, professional advice and insurance. It also makes a real difference to people in their daily lives, helping them save for the future, buy a home, invest in a business and manage risk.

We welcome the opportunity to respond to 'Operational Incident and Third Party Reporting' from the Financial Conduct Authority (FCA) (CP24/28), 'Operational Resilience: Operational Incident and Outsourcing and Third-Party Reporting' from the Prudential Regulation Authority (PRA) (CP17/24). While we have structured our response in line with the questions posed by the FCA, this sets out our key considerations in response to both CP23/28 and CP17/21, as well as the Bank of England's (BoE) proposals for financial market infrastructures (FMIs). Some of our comments specifically address specific proposals from one regulator. However, we ask that the FCA, PRA and BoE (collectively "**the regulators**") take these into consideration.

Summary

We support the intention behind these proposals and welcome the regulators' efforts to improve their oversight of potential operational and third-party risks through more structured, consistent and effective reporting requirements. However, we do not support the proposals as currently drafted. At present, the proposals are too ambiguous and overly complicated and would, therefore, result in the overreporting of low-level incidents, an unnecessary level of intermediate reports and initial triaging and duplicative reporting requirements. This would place a disproportionate burden on firms.

The current proposals also risk creating duplication with existing requirements, and in certain instances the purpose or value of some of the proposed reporting is unclear. The regulatory reporting burden has already increased considerably in recent years, creating a major operating friction for UK firms and we strongly encourage that the focus of additional requirements should be on reporting that is genuinely useful for supervision.

Overall, we believe the proposals as currently drafted fall short of meeting the regulators' secondary objective for international competitiveness and growth. The regulators should re-assess their proposals, as outlined below, to ensure they are fit to enable and enhance the future competitiveness of the UK financial sector.

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?

We believe that the stated benefits to firms expressed within the Cost Benefit Analysis (CBA) are over-estimated. The FCA and PRA have provided two separate criteria where there is inconsistency between the PRA's financial stability threshold and the consumer harm threshold of the FCA. We believe this conflation, alongside the addition of subjective analysis included in the assessment criteria (operational contagion, indirect impact, potential incidents, sector/client/consumer impact), will result in a material ongoing cost due to the increased disconnection between regulatory reporting and incident management.

We have concerns regarding the continued reference to 'monitoring market-wide risks' and using the incident data to enable future work. Incident reporting, during the period of incident management, should be based on informing regulators and supervisors regarding actionable information that is relevant to the individual incident. Incident reporting for the purposes of data collection, market analysis and trends is of minimal benefit to the sector, given that there are other forums where the regulators can request this information (see our response to question 3). Intervening in incident management for data collection misallocates resources away from remediation and management.

The regulators should acknowledge that the costs of both incident reporting and third-party proposals are not one-offs but include the ongoing compliance costs of annual reporting. For example, the regulators propose to require firms to maintain and submit a structured register of information on all their material third-party arrangements. While the PRA suggests that firms can 're-upload the Register in its entirety' on an annual basis, in reality, firms will need to review and update this.

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

While firms will already have well-established incident reporting processes, including the classification of incidents, steps to more clearly define what constitutes an 'operational incident' for reporting purposes are positive. However, the current definitions remain too broad. The proposed definition would potentially capture any incident and require firms to apply these terms too broadly, leading to an overly burdensome approach to compliance. The regulators should provide clarity on the scope of 'users external to the firm'.

We are also concerned by the lack of a materiality lens within the definition, and that firms could be required to assess the impact of an incident on data held at third-party providers.

Firms often cannot access such information, and this should instead be covered by the 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?

We support the regulators' intention in setting reporting thresholds for operational incidents. However, we do not support the current thresholds, which would create a disproportionate reporting burden for firms. A proportionate approach to reporting is essential to prevent compliance burdens from stifling innovation and to enable institutions of different sizes and business models to compete on equal footing. This is central to the regulators' secondary objective for international competitiveness and growth. Several features of the current proposals need to be amended to ensure proportionality.

The current reporting thresholds are too ambiguous and subjective, particularly regarding alignment with Important Business Services (IBS) and the capture of near misses. We do not support the inclusion of terms and criteria such as what 'could' occur, operational and financial 'contagion', 'indirect impact' and, in the extreme, reporting in relation to an incident that has yet to occur. Such terms require firms to undertake subjective analysis of the wider impacts and make the proposals disconnected from the incident management of regulated firms. The FCA's use of "could" in 'could cause or has caused intolerable levels of harm to consumers' is too ambiguous as, at the time of occurrence, firms cannot be sure of the full future impact of the incident; any incident could, in theory, result in intolerable harm. This may lead firms to overreport minor incidents or spending a disproportionate level of full-time equivalent (FTE) work determining 'if' an incident – including even a theoretical incident- should be reportable. This would divert key resources from managing genuinely significant disruptions and creating disproportionate compliance burdens.

Disproportionate and superfluous reporting requirements for minor incidents would overburden firms and run counter to the regulators' legal duty to promote economic growth as part of the secondary objective established in the Financial Services and Markets Act 2023 (FSMA 2023). The regulators should simplify and more clearly define the reporting thresholds, while removing any subjective criteria. In particular, the FCA should establish a more specific requirement than 'could cause or has caused intolerable levels of harm to consumers'. The regulators should also streamline the thresholds to focus on only the most critical incidents impacting the UK markets and consumers. We encourage the regulators to limit reportable operational incidents to those that have already occurred and demonstrate confirmed or actual impact.

The FCA should align with the PRA/BoE by recognising a firm's internal classification of an operational incident as a relevant factor in determining whether the incident meets the reporting threshold. A firm's internal classifications align with the existing UK operational resilience regime and the thresholds of each regulator. Classifications will include a firm's

thresholds to determine the severity of impact, which will be directly related to the other assessment criteria proposed by the FCA (such as the ability to provide services, impact on the firm's clients and data loss). A lack of a standardised approach to the assessment criteria for incident reporting would result in incident triages requiring assessment across the regulators, diminishing the benefit of one incident reporting format. Ensuring the regime is as connected as possible to a firm's internal incident management process should be a key priority of both regulators.

While the case studies provided by the FCA are helpful in illustrating how firms should apply the reporting thresholds, this causes inconsistencies in how the different regulators interpret incident criticality. This includes an example whereby an incident could have an impact on 'some' clients, that introduces an impact to any aspect of 'day-to-day management', or a website being taken offline for an undetermined period without consideration of alternative banking services being provided by an app, Post Office or via phone. There is, in addition, a significant criticality difference between the outage of an online-only digital bank's IT infrastructure (in case study eight) versus case study five with a website being offline. We are concerned that the 'consumer harm' criterion has been interpreted widely and become disconnected from the operational resilience regime where it has already been defined and connected to IBS. While we understand and support the FCA's intention in proposing case studies, intolerable harm is particular to each financial institution and cannot be rectified within blanket case study descriptions. The FCA should reconsider these case studies using an outcomes-based focus to illustrate where a firm has been able to use its own internal classifications of the incident.

We are also unclear on the regulators' objectives in setting the incident reporting thresholds. Some of the purposes outlined for incident reporting veer away from actionable intelligence and towards broader data collection. As noted in response to question 1, the latter would not be a sufficient reason to divert resources away from incident management, during or in the immediate aftermath of a disruption. There are also existing, better-placed tools for authorities to gather information and insights on the wider impacts of an incident, such as the Sector Response Framework and the Cross Market Operational Resilience Group (CMORG). The regulators should clarify how these align and their intention for the use of the data during an incident and the subsequent purpose of data collection.

The regulators should base the incident reporting regime on the existing operational resilience regime applicable in the UK and consider where the proposed rules overlap with existing rules to avoid duplication. For example, the requirements under SUP 15.3 and SYSC 15A.2.11G in the FCA Handbook, or Payment Services Directive 2 (PSD2) incident reporting.
We recommend 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. Therefore, we 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 a single reporting approach in the UK. While PSD2 reporting figures are low, the continued use of an alternative classification within firms causes a significant operational burden for each payments-related incident, with members noting approximately 7-1 triages per reported incident. Each triaged incident would face impact assessments according to the PSD2, FCA and PRA assessment criteria, both at the initial analysis of the incident and for the initial reporting thresholds. This is highly complex and adds disproportionate burdens to each payments incident, notwithstanding the regular numbers of requests for information which firms face after submission.

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

We support a standardised approach to reporting and the regulator's intention in creating more structured and consistent incident reporting across the industry. However, the regulators current approach needs to be finetuned. If retaining Principle 11 or Fundamental Rule 7 reporting, firms should only be required to report in one format, to ensure they are not required to report on the same incident twice. The initial report also has fields that require review and approval from the same people handling the operational disruption, potentially diverting resources from incident management to regulatory compliance.

The PRA/BoE proposals require firms to submit an initial report within 24 hours of identifying an operational incident. While we do not oppose this in principle, many details may still be unknown at this stage and trying to gather this information may divert attention from investigating and responding to the issue. The PRA/BoE should clarify what 'limited information' is expected at this stage, how this relates to the existing reporting of incidents directly to supervisory teams and be explicit that they do not expect firms to redirect critical resources away from managing the incident to supply this initial report. The benefit provided to firms from an incident reporting regime would be to allow structured information exchange, instead of requests for information-based interactions with exceptionally short timelines and inconsistent information requests.

While we support the standardisation of incident reporting, the current divergence in the regulators' approaches undermines this goal. The regulators should align their individual reporting requirements and consider any unintended consequences of how they interact. The registers for each regulator should be completely aligned at every level. Currently, these diverge in both definitions and some of the fields, which capture the same information but with different numbering or wording. These misalignments are unhelpful and not only create an unnecessary operational burden for firms but will also pose a transposition burden for the regulators should they need to share the information. To ensure consistency, reduce duplication, and achieve effective standardisation, the regulators must establish joint definitions and approaches, while removing duplicate regimes (PSD2, Principle 7 and 11 reporting).

The regulators propose a 30 working days deadline for the final incident report or, recognising that some incidents are complex and may require detailed investigation before a final report can be submitted, 'as soon as is practicable but not exceeding 60 working days' where 30 days is impracticable. Financial entities often will not complete the final review of an incident within a 6-week timeline. This is due to the collection of all relevant information across multiple lines of business and the administrative time and governance required to undertake full analyses of root causes. Reviews are undertaken across numerous teams, include all lines of defence and are signed off by senior executives, which can all push full reviews beyond 30 working days. Therefore, we support a standard 'as soon as practicable' deadline instead of a 30- or 60-day statement. The regulators have not provided a satisfactory justification for the proposed deadline.

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?

No, while we support the regulators' intentions, we do not agree that the current proposals are sufficiently proportionate. Please refer to our answers to questions 1-4.

Following an incident report, regulated firms are often subject to considerable supervisory requests and the type of data and granularity of that data can often vary across incidents. Further clarity is needed on how the regulators will respond to incident reports at the various stages of the reporting process (initial, intermediate, and final). The regulators should also take a coordinated approach to engaging firms, following an incident report, to minimise the risk of firms receiving multiple requests for the same issue. A single communication channel between the regulator and the firm following an incident would help manage the regulators' follow-up questions more efficiently and reduce the burden on firms. Greater consistency in information requests would help firms anticipate requirements and provide more useful information.

We welcome efforts to align these proposals with other jurisdictions' reporting regimes and international standards, such as the Financial Stability Board's (FSB) Format for Incident Reporting Exchange (FIRE). Where possible, establishing a single baseline set of operational resilience regulations is key to minimise compliance burdens for global firms. The regulators should take lessons from the European Union's (EU) Digital Operational Resilience Act (DORA) implementation both regarding replicating the positives, like removing duplicate obligations and avoiding the negatives, for example complex subcontracting and register requirements. The current FCA proposals require firms to consider whether an operational incident could result in failure to meet their legal and regulatory obligations, despite the final version of DORA omitting similar requirements following industry consultation. Firms should not be required to comment on legal exposure within reporting when the full information may not be available.

Smaller firms could be disproportionately burdened by these new rules. Unlike firms already within the scope of PS21/3, they have not been subject to the same level of reporting or supervisory expectations around operational resilience. Therefore, if the FCA proceeds with its proposal to extend the rules in Chapter 3 to all firms, it is crucial that they allow adequate time for the implementation of the new rules and changes.

Finally, the sheer number of parallel live consultations on additional incident reporting requirements (FCA CP24/28, PRA CP17/24, the BoE's FMIs proposals and the Home Office's consultation on ransomware reporting requirements) illustrates the overreporting burden that could arise for firms. CP24/28 and CP17/24 are, in effect, four separate consultations. The FCA and PRA/BoE proposals could have better achieved their aims while supporting proportionality through two joint consultations, one on incident reporting and the other on third-party reporting.

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

We accept the regulators' aligned definition of third-party arrangements.

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

We support the regulators' proposed definition as clear, risk-based and proportionate. A materiality threshold within the scope of third-party arrangements is key to ensure the right balance between effective regulation and operational efficiency.

However, a common definition and closer alignment on the factors for determining materiality would simplify already complex compliance processes for firms. This would be more in line with the regulators' secondary objective.

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 support better alignment between the FCA and PRA/BoE approaches to material third-party notifications. While we understand that the PRA/BoE's intentions in providing greater specificity than 'all material third-party arrangements' ('due to the associated risks, necessitates a high degree of due diligence, risk management or governance by the firm'), this adds unnecessary complexity and creates misalignment with the FCA approach. This creates an unnecessary operational burden, making it difficult for firms to create a single supporting process. The PRA/BoE should align with the FCA's definition, leaving the determination of the materiality of arrangements to the firm's judgment.

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

DORA has highlighted complications from excessive reporting requirements for subcontracting, which are operationally challenging for firms to implement. Maintaining the DORA registers of information is another significant burden, for example the complex data fields and data gathering required. Wherever possible, the regulators' templates for third-party reporting should be compatible with the FSB FIRE, allowing firms to build on their existing work rather undergoing the burdensome task of reassessing all their third-party providers. Firms face challenges maintaining multiple registers and complying with expanded regulatory scopes, including non-outsourcing arrangements. Streamlining and simplifying regulatory notification requirements (for new arrangements and registers) is essential to alleviate this burden.

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

A significant challenge faced by financial firms is the lack of transparency and information sharing from certain third-party providers, particularly those that are global players - in particular global custodians, web service (including cloud) providers, 'Big Tech' firms and market data providers. This lack of transparency can range from, at best, minimal information provided - such as excerpts from a manual – to, at worst, no information at all. This may limit firms' ability to provide all the information required.

Other comments

We would welcome further details from the regulators on how the proposed incident reporting requirements would be managed in a system-wide scenario. For example, if these proposals had been in place during the 2024 CrowdStrike incident, the regulators could have thousands of similar incident reports all at once. Not only would the collective effort required by firms to complete incident reports divert resources from managing the incident directly, but it is difficult to see how the regulators would be able to usefully digest this volume of similar information. We would support a mechanism for regulators in such instances to signal to firms that regulators are aware of the incident and that it does not require further incident reporting.

Conclusion

TheCityUK supports steps by the regulators to strengthen cross-industry resilience by providing a more structured and consistent approach to incident and third-party reporting requirements. However, the proposals set out in CP23/30, CP26/23 and the BoE's FMIs consultation require further refinement to ensure proportionate, aligned and effective final reporting rules. We look forward to receiving clarity on the areas outlined above and, in due course, the final rules from the regulators.