NEW OPERATIONAL RESILIENCE REQUIREMENTS FOR PAYMENT FIRMS

Date: 1 June 2021

UK Policy and Regulatory Alert

By: Kai Zhang

Following a consultation in 2019 (CP19/32),[1] the Financial Conduct Authority (FCA) has now published its policy statement (PS21/3) and final rules on operational resilience.[2] The FCA has stated that the new rules on operational resilience are not intended to conflict with or supersede existing requirements on firms to manage operational risk or business continuity planning, but rather, to set new requirements that will enhance the resilience of in-scope firms.[3] In this regard, the FCA has commented that the pandemic has shown why it is critically important for firms to "understand the services they provide and invest in their resilience."

Broadly, the new rules require that payment firms, and other in-scope firms, must, on a proportionate basis having regard to the nature, scale, and complexity of the firm's activities, set "impact tolerances" for their "important business services" and that they must then remain within such impact tolerances in the event of a severe but plausible operational disruption, including such disruption that is outside of a firm's control, e.g., a computer virus attack.

The new rules, which will be set out in a new chapter (SYSC15A) to be added to the Senior Management Arrangements, Systems and Controls sourcebook of the FCA Handbook, will formally apply from 31 March 2022. However, in-scope firms are reminded that they should begin identifying "important business services," "impact tolerances" (see below), and vulnerabilities in operational resilience from 31 March 2021 and complete this exercise by the in-force date; then, firms must, as soon as reasonably practicable, and in any event within three years of the rules coming into force (i.e., by 31 March 2025), have performed mapping (i.e., developing a clear picture of the resources that enable an important business function to run and the impact of disruption) and testing and made necessary investments to enable them to operate consistently within their "impact tolerances."

AFFECTED FIRMS

The new rules apply to, amongst others, payment institutions (both authorised and small) and electronic money institutions (both authorised and small), but only with respect to the provision of regulated payment services and issuance of e-money (respectively) and activities connected thereto.[4] On this basis, a hybrid payment institution with separate non-payment business would not need to comply with the new rules in relation to the non-payment business (to the extent that the business is not connected to its regulated payment services).

For brevity, we use "payment firms" herein to refer collectively to payment institutions and electronic money institutions.

While the rules do not only cover payment firms, and, for example, will be relevant for banks and enhanced scope senior managers' and certification regime (SM&CR) firms, we focus on payment firms in this article.

IMPORTANT BUSINESS SERVICES

An “important business service” for these purposes means a service that, if disrupted, “could (1) cause intolerable levels of harm to customers; or (2) pose a risk to the soundness, stability or resilience of UK financial system or the orderly operation of the financial markets.”

The rules include various factors that can be considered by payment firms, and other in-scope firms, for the purposes of identifying their “important business services,” such as the nature of the firm's customers, the ability of customers to find replacement providers, the sensitivity of data, the impact on the payment firm's financial position, the potential of reputational damage, and the potential for knock-on effects.

Payment firms only need to identify “important business services,” not all business services, and for these purposes, this covers only services provided to external customers.

There is no need to identify products. For example, for an EMI, the provision of access to e-money wallets to initiate payments would be a service, but not the wallet itself, which is a product.

Payment firms must identify “each” of their important business services, not a “collection” of services. The FCA gives some examples of what these mean (albeit the examples are for the banking sector): accessing an online mortgage account and telephone mortgage banking are two separate services, whereas the provision of mortgages is a collection of services.[5]

IMPACT TOLERANCE

The term “impact tolerance” refers to the maximum level of disruption that can be tolerated without the “harm” or “risk” (as mentioned in the “important business service” definition) materialising. An impact tolerance must be set for each important business service. Note that there are no prescriptive criteria or a definition for “intolerable harm.” But in the FCA's view, it generally means harm from which customers cannot easily recover.

Such impact tolerances must be set by reference to “a length of time” (other metrics can also be used, but must be used together with the duration metric). That is, an important business service must not be disrupted beyond a certain period of time or point in time; any further disruption beyond such period/point would cause the said “harm” or “risk.”

For example, in an example given by the FCA, an electronic money institution might set an impact tolerance of 2 hours of unavailability in relation to access to the firm's e-money wallet.

Payment firms should consider European Banking Authority's Guidelines on ICT and Security Risk Management[6] when setting their impact tolerances.[7]

OTHER REQUIREMENTS

There are also other requirements in relation to the relevant internal procedures and processes payment firms must set up in order to comply with the rules. These include requirements to:

- have comprehensive and effective strategies, processes and systems to comply with the rules;
- have a testing plan, to assure the firm can remain within the impact tolerance for each important business service;

- conduct testing regularly in a range of severe but plausible scenarios;
- maintain an internal and external communication strategy, e.g. informing customers of operational disruptions; and
- make, and keep up-to-date, a self-assessment document in relation to their compliance with the requirements.

CONCLUSION

The new regime demonstrates that the FCA is increasingly turning its attention to the payment sector. This can be seen from the fact that, other than payment firms, the new regime only applies to enhanced scope SM&CR firms, banks, PRA/FCA dual-regulated investment firms, building societies, insurers and investment exchanges, in other words, mostly large and complex firms. However, all payment institutions and electronic money institutions of all sizes are subject to the new requirements, albeit that the new rules do envisage an approach to compliance which is proportionate to the nature, scale, and complexity of a firm's activities.

FOOTNOTES

[1] CP19/32 (December 2019), https://www.fca.org.uk/publication/consultation/cp19-32.pdf.

[2] PS21/3 (March 2021), https://www.fca.org.uk/publication/policy/ps21-3-operational-resilience.pdf.

[3] PS21/3, para. 1.11.

[4] SYSC15A.1.8R (forthcoming 31 March 2022), https://www.handbook.fca.org.uk/handbook/SYSC/15A/1.html?date=2022-03-31.

[5] PS21/3, para. 2.4.

[6] EBA/GL/2019/04 (29 November 2019), https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/872936/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf.

[7] SYSC15A.2.12G (forthcoming 31 March 2022), https://www.handbook.fca.org.uk/handbook/SYSC/15A/2.html?date=2022-03-31.

KEY CONTACTS

KAI ZHANG
SPECIAL COUNSEL

LONDON
+44.20.7360.6404
KAI.ZHANG@KLGATES.COM

PHILIP J. MORGAN
PARTNER

LONDON
+44.20.7360.8123
PHILIP.MORGAN@KLGATES.COM

JUDITH RINEARSON
PARTNER

NEW YORK, LONDON
+1.212.536.3928
JUDITH.RINEARSON@KLGATES.COM

