


How ‘operational resilience’ enables compliance with the ‘consumer duty’ and ‘vulnerable customers’

24 November 2023  Jeremy Irving

This article was first published by Thomson Reuters.

Part 3: Intolerable harm

This is the third and final article aiming to highlight how, across different financial services industries, Operational Resilience (“O.R”), the Consumer Duty (“CD”) and Vulnerable customers (“VC”) frameworks are inter-linked, with failings under one such regime likely echoing in the others.

This article considers the meaning of the rule at SYSC 15A.2.1R (“A firm must identify its important business services”) by reference to the second test it contains, which is whether disruption to the service could “pose a risk to the soundness, stability or resilience of the UK financial system or the orderly operation of the financial markets” (referred to below as “macro risk”).

The essentials

Some guidance on the nature of a macro risk is at SYSC 15A.2.4:

“The factors that a firm should consider when its important business services include, but are not limited to:

- (4) the number of clients to whom the service is provided ...
- (6) potential to inhibit the functioning of the UK financial system;
- (7) the firm's potential to impact the soundness, stability or resilience of the UK financial system;
- (8) the possible impact on the firm's financial position and potential to threaten the firm's viability where this could ... pose a [macro] risk ...
- (9) the potential to cause reputational damage to the firm, where this could ... pose a [macro] risk ...
- (12) the potential to cause knock-on effects for other market participants, particularly those that provide financial market infrastructure or critical national infrastructure; and
- (13) the importance of that service to the UK financial system, which may include market share, client concentration and sensitive clients (for example, governments or pension funds).”

The Bank of England / Prudential Regulation Authority (collectively, “PRA”) and Financial Conduct Authority (“FCA”) joint policy summary, “Building operational resilience ...” states that the PRA sets out in “its Financial Stability Strategy that financial stability is the consistent supply of the vital services that the real economy demands from the wider financial sector. ... providing the main mechanism for paying for goods, services and financial assets; intermediating between savers and borrowers, and channelling savings into investment, via debt and equity instruments; and insuring against and dispersing risk.”

In its [2018 Discussion Paper](#), the PRA gives further examples of macro risk crystallisation in the “payments network” and the aggregate effects of attempted mitigants or controls resulting in “significant gridlock in processing payments; reduc[tion of] overall liquidity in the financial markets; and ... a build-up of unsettled positions and bilateral credit exposures among financial institutions ... [which] could ultimately impede economic activity and disrupt financial stability.” In other words, although this phrase is not used in the above, ‘contagion risk’.

Practical considerations

It may seem obvious that macro or contagion risks could engage issues of customer vulnerability and even raise questions as to the ineffectiveness of systems and controls amounting to a breach of [PRIN 2A.2.8 R](#) (“A firm must avoid causing foreseeable harm to [retail customers](#)”).

However, on a practical basis, many firms might make a general assumption that they are far from being capable of causing or contributing to such risks. The accuracy of such assumption is significant because this will inform how firms go about complying with SYSC 15A.5.3 R: “A firm must carry out scenario testing, to assess its ability to remain within its [impact tolerance](#) for each of its [important business services](#) in the event of a severe but plausible disruption of its operations.” Establishing such ‘plausibility’ involves:

- identifying “an appropriate range of adverse circumstances of varying nature, severity and duration relevant to its business and risk profile” (SYSC 15A.5.4 R); and
- considering all attributes of a scenario including:
 1. “corruption, deletion or manipulation of data ...
 2. unavailability of facilities or key people ...
 3. unavailability of third party services ...
 4. disruption to other market participants ...
 5. loss or reduced provision of technology ...” (SYSC 15A.5.6 G).

More concrete practical guidance on the nature of a macro-risk, and how it can affect a firm’s ability to comply with the CD and deal appropriately with VCs, can be found in the December 2022 [final notice from the PRA to TSB Bank](#).

In April 2018, TSB migrated the majority of the operations of its corporate systems, customer services and customer data to a new IT platform. TSB encountered serious issues which significantly affected many customers’ use of their accounts, including data breaches, failures with digital (internet and mobile) banking services, failures in telephone banking, branch technology failures, and consequential issues with payment and debit card transactions.

TSB received 225,492 complaints and paid a total of £32,705,762 in redress, including distress and inconvenience payments.

At the time, TSB was positioning itself as a “challenger” to the established high street banks. At the outset of the migration programme, the PRA notified TSB that “while the impact of any operational failure on TSB’s brand was unknown because of the lack of other examples [of similar scale migrations] to date, [the PRA] had a concern that the result could potentially be more severe for TSB’s recently established brand as a challenger bank if customers felt that it impacted their confidence in TSB’s safety and soundness.”

As the PRA later explained in the final notice “As a challenger bank, TSB was potentially more vulnerable to brand damage arising from operational failures and therefore at risk of loss of confidence ... leading to potential depositor outflows ... [These] could also impact confidence in challenger banks more broadly, and therefore potentially have a negative impact on financial stability.” This suggests that UK regulators are willing to consider macro risks as on a ‘peer’ or market-reputational contagion basis. This approach could be relevant to many sectors.

The FCA also issued a [Final Notice](#) against TSB for breaching Principles 2 (conducting business with due skill, care and diligence) and 3 (taking reasonable care to organise and control the migration programme responsibly and effectively) by failures in its –

- engagement with the associated company that handled the programme and its sub-contractors;
- preparations and risk management for the migration, especially testing and “an excessively ambitious timetable”; and
- governance, in particular: “It [did] not appear certain matters were sufficiently discussed with or challenged by the TSB Board, such as the timetable for the migration ...”

It is also worth noting that while the above notices did not explicitly seek to rely on or highlight the regulators' operational resilience regime, the April 2023 [Final notice from PRA to Carlos Abarca](#), who had been the Chief Information Officer of TSB in the run up to and during the IT migration, did do so. The need to prevent foreseeable harm as per the CD is at least implicit in the text of the relevant notice, in that the PRA noted that Mr Abarca was "the owner of the material risk that 'migration causes ... poor customer outcomes' under TSB's Material Risk Register."

While it is not an explicit feature of the OR, CD or VC frameworks, the concept of 'contagion risk' was explicitly identified in the 2014 fine of [RBS group](#) which involved similar circumstances to the TSB fine: an IT outage risked multiple banks "not being able to carry out their core functions [which] ... could have affected financial stability ... [via] ... credit and liquidity exposures between settlement banks and the indirect participants that use their services ..."

Key contact



Jeremy Irving

Partner

jeremy.irving@brownejacobson.com

+44 (0)20 7337 1010

Related expertise