Regulators Get Tough on Regulatory Outsourcing Failings

Latest FCA and PRA fines against a retail bank show little tolerance for poor outsourcing systems and controls.

On 29 May 2019, the FCA and PRA announced that they had fined an independent UK bank for failing to manage its outsourcing arrangements properly between April 2014 and December 2016. The bank received separate fines of £775,100 from the FCA and £1,112,152 from the PRA (resulting in a combined fine of £1,887,252) for breaches of the regulators' high-level principles for authorised firms, as well as their more detailed rules on outsourcing. Each fine includes a 30% early settlement discount.

The bank was fined by both regulators as the failings resulted in breaches of both regulators' rules, and went to both regulators' statutory objectives (specifically, the FCA's consumer protection objective and the PRA's objective to promote firms' safety and soundness). Although both regulators applied the same five-step penalty framework to calculate their penalties, the way in which they applied the framework led to different figures. In particular, because the PRA had previously fined the same bank for outsourcing failures in November 2015, the repeat failure was a significant aggravating factor that led to an uplift in the PRA's penalty.

What Went Wrong?

The firm in question is a retail bank operating prepaid card and charge card programmes across the UK and Europe via its payment services division, which relied heavily on a number of outsourced service providers, including reliance on third-party card processors for the authorisation and processing of card transactions.

The FCA and PRA jointly found that the bank failed to establish adequate processes to enable it to understand and assess the business continuity and disaster recovery (BCDR) arrangements of its outsourced service providers, in particular, how those providers would maintain support of the bank's card programmes during a BCDR event. This failure was found to pose a risk to the bank's operational resilience and expose its customers to a serious risk of harm, which crystallised on 24 December 2015, when a technology incident at a card processor led to the unavailability of authorisation and processing services for over eight hours. This incident impacted 3,367 of the bank's customers, who were unable to use their cards at point of sale terminals, ATMs, or online during the peak Christmas shopping period. The regulators took the view that, as the bank had not adequately planned for the risk of such disruption, it was unprepared to manage how it could restore services to its customers.

The FCA and PRA found that the bank's specific failings in relation to the incident resulted from "deeper flaws in its overall management and oversight of outsourcing risk, from Board level down", including weaknesses that had existed (of which, said the regulators, the bank ought to have been aware) since April 2014, and which were not remedied until late 2016, including:

- A lack of adequate consideration of outsourcing within its board and departmental risk appetites
- An absence of processes for identifying critical outsourced services
- Flaws in the bank's initial and ongoing due diligence of outsourced service providers

More specifically, the regulators found that the bank:

- Did not clearly articulate its risk appetite and tolerance levels in relation to the outsourcing of critical services. This meant that it could not determine when its critical outsourcing arrangements exceeded the level of risk it was willing and able to accept.
- Had an outsourcing policy that did little more than recite the general regulatory requirements, and had no process in place for identifying its critical outsourced services. Staff were given no guidance on how to identify critical outsourcings, or how these should be distinguished from non-critical outsourcings.
- Did not put appropriate service-level agreements in place as part of its contractual arrangements with critical outsourced service providers.
- Had BCDR plans that focussed only on services performed directly by the firm, notwithstanding its heavy reliance on outsourcing arrangements. In particular, its BCDR plans did not contain any actions or procedures relating to the continuity and recovery of outsourced services during a disruptive incident.
- Did not consider BCDR arrangements adequately as part of its original due diligence on outsourced service providers, or monitor such arrangements adequately on an ongoing basis. For example, the firm had no policy on what information should be requested from service providers, nor any guidance or criteria for assessing business continuity plans, so they were not reviewed against clear requirements.
- Did not consider how its outsourced service providers' business continuity arrangements would support the continued operation of its card programmes during a disruptive event, or the impact that disruption to these services might have on the firm or its customers.
- Did not respond appropriately to an IT incident at the same provider that preceded the incident in question. The earlier incident prompted only a limited inquiry into the provider's business continuity arrangements and did not result in any changes to those arrangements.

These failings emphasise the importance of establishing proper outsourcing systems and controls. The regulators reinforced the position that the firm remains ultimately responsible for the provision of services by outsourced service providers. In particular, the decision serves as a reminder to regulated firms to ensure that they:

- Put in place and maintain appropriate processes for identifying and monitoring critical outsourcing arrangements. In particular, outsourcing policies should do more than just recite general regulatory requirements — they should be tailored to the firm in question and structured in such a way that the varying risks posed by the outsourcing of different functions are properly addressed.
- Engage in appropriate initial and ongoing due diligence/audits of outsourced service providers to ensure their ability to enable the entity to meet its regulatory requirements throughout the life of the outsourcing arrangement (from request for proposal phase to exiting the outsourcing arrangements and everything in between).
- Ensure appropriate risk identification reporting and management (including BCDR risks) and involve board and other senior management in such processes from the outset.
- Ensure that any weaknesses identified in the outsourcing processes are monitored, reported, and remedied as soon as possible.

Senior Managers

Although no individuals were fined in this case, both regulators took the opportunity to emphasise the important role of senior managers. One of the actions within the bank's remediation plan was to allocate first-line responsibility for the firm's outsourcing arrangements to a senior manager. Banks are now required to do this under the Senior Management and Certification Regime (SMCR). The individual with this responsibility will be accountable for the firm's overall outsourcing policy and strategy, as well as for the firm's compliance with regulatory outsourcing requirements.

The PRA indicated that effective oversight of outsourcing by senior management includes:

- Identifying and understanding the firm's reliance on critical service providers
- Setting proper risk tolerances that are appropriately cascaded
- Ensuring that the firm's risk appetite is adhered to both within the firm and by critical outsourced service providers

While the failings in this case largely pre-date the SMCR, firms can expect that if any such failings were to occur now, the regulators would look to hold the relevant senior manager(s) to account. This could result in the relevant individual(s) facing financial penalties or even having their regulatory approvals withdrawn.

Operational Resilience

How firms manage outsourcing risk is a significant concern for the regulators. So-called "operational resilience" remains a key focus area, having featured prominently in both regulators' Business Plans for 2018/19. The regulators plan to publish a joint consultation later this year, setting out their proposed policy on how they plan to supervise operational resilience. The FCA also plans to look at firms' management of third-party service providers as part of its supervisory work over the coming year.

Firms can therefore expect more attention in this area, as well as further articulation of regulatory expectations. There is also a renewed focus on outsourcing arrangements as a result of the EBA's new outsourcing guidelines, which will come into effect on 30 September 2019 and introduce heightened regulatory expectations in various areas.

Contacts

Fiona M. Maclean

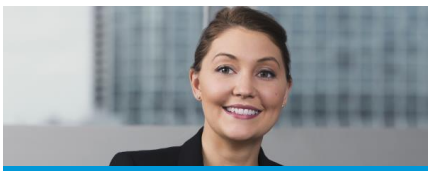
Technology Transactions
Partner, London

T +44.20.7710.1822
E fiona.maclean@lw.com

Christian F. McDermott

Technology Transactions
Partner, London

T +44.20.7710.1198
E christian.mcdermott@lw.com



Laura Holden

Technology Transactions
Associate, London

T +44.20.7710.1802
E laura.holden@lw.com

Charlotte Collins

Knowledge Management Lawyer, London

T +44.20.7710.1804
E charlotte.collins@lw.com