Bank Technology Failures:
A New Frontier for Regulatory Intervention?

Gavin Smith and Simun Soljo examine the consequences – in the UK and Australia – of a failure by regulated institutions to have adequate systems and controls in place to prevent the occurrence of a serious IT incident.

INTRODUCTION

In an unprecedented and ground-breaking move, the UK's Financial Conduct Authority (***FCA***) and Prudential Regulatory Authority (***PRA***) have fined three RBS group banks a total of £56 million, over A$100 million, for failing to have adequate systems and controls to prevent the occurrence of a serious IT incident in 2012. The fines were imposed following the occurrence of widespread and well-publicised problems with RBS's IT systems affecting more than 6.5 million customers in the UK in June 2012.

The fines are the largest ever imposed in Europe for technology failures in the financial services industry and serve as a cautionary tale for Australian financial institutions. What obligations do regulated financial institutions in Australia have to put in place adequate IT systems, and what action could the Australian regulators take for similar technology failures?

The fines are the largest ever imposed in Europe for technology failures in the financial services industry and serve as a cautionary tale for Australian financial institutions. What obligations do regulated financial institutions in Australia have to put in place adequate IT systems, and what action could the Australian regulators take for similar technology failures?

BACKGROUND TO FCA ACTION

In June 2012, the IT team at RBS in the UK implemented an upgrade to the software that processed updates to customer accounts. A simple step undertaken regularly by banks all round the world. But the upgrade didn't run to plan so the IT team uninstalled it.

What happened next was far from routine. 6.5 million customers of RBS and its subsidiaries Natwest and Ulster Bank woke up to discover they were unable to use online banking facilities or access accurate account balances at ATMs; they were unable to pay their mortgages on time and were left without cash while on vacation. The banks also found themselves unable to apply correct credit and debit interest to customer accounts or to produce accurate account statements. Some companies were unable to pay salaries to employees or finalise their accounts for audit purposes. The RBS banks were also unable to participate in the broader clearing system. Major problems continued for several weeks and the RBS banks were forced to manually update account balances.

The resulting investigation and enforcement action into the incident marks the first time that the FCA and the PRA have acted together. In its final notice to the RBS banks, the FCA found that the RBS banks breached Principle 3 of the FCA handbook. Principle 3 requires regulated institutions to take reasonable care to organise and control their affairs responsibly and effectively, with adequate risk management systems. In this case, the FCA found that the RBS banks did not have adequate systems and controls to identify and manage their exposure to IT risks. The FCA highlighted the following three issues in particular:

- there were inadequate testing procedures for managing changes to software;
- the risks related to the design of the software system that ran the updates to customers' accounts were not identified;
- the IT risk appetite and policy was too limited because it should have had a much greater focus on designing systems to withstand or minimise the effect of a disruptive incident.

The FCA's decision is particularly interesting because it marks a subtle but significant change in applying regulation with the purpose of ensuring banks are able to recover from disruptions, to a new focus of ensuring that banks have the resilience to be able to withstand the effect of disruptions. The FCA describes this as a shift away from 'business continuity' to 'resilience'. UK financial institutions should expect to see the latter term used considerably more in the future.

> ***the FCA found that the RBS banks did not have adequate systems and controls to identify and manage their exposure to IT risks***

Since the incident in 2012, the FCA has also used its 'Dear Chairman' function to conduct an assessment across the UK banking sector to determine how well they are managing their exposure to IT risk and the extent to which they have themselves audited their vulnerability to technology failures which might affect their retail functions. This has been a detailed and burdensome exercise for the banks.

Both the FCA and PRA reduced their fines by 30 per cent on the basis that RBS agreed to settle at an early stage. But for that action, the fines would have been even higher. Australian institutions should note that the A$100 million fine is also just part of the picture. RBS was also

>

Bank Technology Failures: [CONT'D]

> forced to make a £125 million (A$230 million) provision available to account for financial costs and expenses arising out of the incident. And the reputational damage has been enormous. A very expensive software update indeed.

THE AUSTRALIAN CONTEXT: AN EQUIVALENT FOR AUSTRALIAN REGULATED INSTITUTIONS?

So, could a similar fate befall Australian regulated entities? The answer is yes and no.

1. AFS licensees

Australian financial services (***AFS***) licensees and APRA-regulated entities are subject to obligations to have in place and maintain adequate IT systems.

The FCA's decision marks a subtle but significant shift away from 'business continuity' to 'resilience'

Specifically, the *Corporations Act 2001* (Cth) requires AFS licensees, other than APRA regulated entities, to 'have available adequate resources (including financial, technological and human resources) to provide the financial services covered by the licence and to carry out supervisory arrangements'. ASIC provides guidance in Regulatory Guide 104 as to how AFS licensees may assess the adequacy of their technical resources. It advises licensees that they need to regularly review their IT systems, including to consider the IT system security, the currency of hardware and software, the quality and relevance of the applications used, and the use of legacy IT systems. Licensees are also required to 'have adequate risk management systems'.

A breach by an AFS licensee of these obligations could result in action by ASIC. It would most likely seek an enforceable undertaking from the AFS licensee requiring the licensee to take remedial action in relation to the breach, but it could also impose additional licence conditions, or suspend or cancel the licence, or seek declaratory relief from the court. Unlike the FCA and PRA, ASIC cannot impose a fine.

2. APRA-regulated entities

The relevant obligations of APRA-regulated entities generally arise under prudential standards issued by APRA.

For example, a registrable superannuation entity (RSE) licensee is required, under APRA Prudential Standard SPS 220 – Risk Management, to 'maintain technical resources at a level adequate for its business operations'. 'Technical resources' are defined to include 'technical systems, including adequate hardware, data quality and software' and 'technical resources to handle any significant changes or increases in size, business size or complexity that are planned, forecast or likely to occur'. Failure to put in place adequate technical systems or to plan appropriately for changing demand on systems could be a breach of the RSE licensee's obligations under the prudential standard. Of course, as is commonly the case, the RSE licensee might obtain access to technical systems by outsourcing the provision of its IT systems or services. If so, the licensee must also comply with the requirements in the Prudential Standard SPS 231 – Outsourcing.

A breach by a trustee of the obligation in the prudential standards is a breach of its licence conditions and may result in a direction from APRA to comply with the requirement (under section 29EB of the Superannuation Industry (Supervision) Act 1993 (Cth) (the SIS Act)). In an extreme case, this could result in cancellation of the RSE licence (under s29G of the SIS Act). APRA does not have the power to issue fines in relation to breaches of the licence conditions.

For ADIs, general insurers and life companies (which are also subject to APRA prudential standards), a major technology failure would most likely be addressed by the obligations in the prudential standard relating to risk management. From 1 January 2015, this will be the common Prudential Standard CPS 220. CPS 220 places a broader, but less technology specific, requirement on ADIs, insurers and life companies to manage their risks and to ensure sufficient resources are allocated to risk management. An incident such as the RBS failure in June 2012 could well attract the attention of APRA in this regard. And if the provision of technology systems or services is outsourced, these entities will also need to comply with APRA's outsourcing requirements set out in Prudential Standard CPS 231 – Outsourcing. A breach of the standard may result in APRA giving the entity a direction under the relevant legislation to comply with the requirement or take other remedial action (a failure to comply with the direction is an offence), or, in the extreme case, a revocation of the licence.

SOME OBSERVATIONS

Although the powers available to ASIC and APRA may not currently match the severity of those available to the FCA and PRA in the UK, the imposition of specific obligations on RSE licensees and AFS licensees nonetheless highlights the need for all regulated entities to address the potential risks posed by their IT systems. If an Australian financial institution suffered the same magnitude of customer-affecting IT failure as RBS, it is highly likely that both ASIC and APRA would seek to follow the precedent set by the FCA and PRA and exercise their powers. Australian institutions should also be mindful of the FCA's shift in focus away from business continuity towards the concept of resilience. Where the UK goes, Australia may well follow.

GAVIN SMITH is a partner and SIMUN SOLJO is a Senior Associate at Allens.