Operational Incidents in Retail Payments Systems: Conclusions

NOVEMBER 2012

Contents

ISBN 978-0-9873620-6-3 (Online)

1. Introduction

Over the past few years, there have been a number of operational incidents in retail payments systems, which became prominent because of the considerable disruption they caused to customers of the authorised deposit-taking institutions (ADIs) in question, as well as to other ADIs and their customers. Such incidents have the potential to dent public confidence in retail payments systems if they result in payment delays and difficulties accessing transaction information.

In all of the most recent cases, the Reserve Bank was aware of and monitored the incidents once it became aware of the problems, and communicated with the affected institutions and industry bodies as appropriate. Although each incident was the product of its own set of unique circumstances, a number were associated with implementing changes to legacy systems. While these systems have proven to be very robust over many years, their advanced age is contributing to operational risk. In some instances, these systems have not been subject to a regular program of renewal and upgrade, and may be vulnerable to ad hoc manual workarounds. Efforts to address the original issue have on occasion caused further problems, suggesting that some institutions' incident management arrangements could be improved. In addition, it is becoming increasingly difficult to ensure the availability of sufficient staff skilled in legacy application languages and with a detailed understanding of the intricacies and interdependencies between component systems.

Given the growing importance of retail payments and the potential system-wide implications of any incident, the Bank has been considering how best to strengthen its oversight of future significant disruptions and contribute to the ongoing integrity of retail payments systems. As an initial measure, in February 2012, the Bank formalised its requirements for the reporting of major retail payments system incidents. The Payments System Board also endorsed the Bank initiating an informal consultation with industry participants on retail operational incidents and the organisation of ADIs' retail payments operations, with a view to developing proposals on additional measures to enhance the resilience of retail payments systems.[1] Meetings with interested stakeholders began in April. In total, 15 parties have been consulted, including the four largest banks.

This paper provides a brief background and describes the major findings of the informal consultation, before going on to summarise the Bank's response, and finally considering additional measures. Based on information gathered through this process, the Board has concluded that at present there is no need for a regulatory response. Indeed, in the Board's view, senior management of individual institutions are primarily responsible for improving the operational resilience of their organisations.

1 See RBA (2012), 'Payments System Issues: Retail Operational Incidents', Media Release 2012-03, 20 February. Available at <http://www.rba.gov.au/media-releases/2012/mr-12-03.html>.

2. Background

Given the Reserve Bank's responsibility for promoting an efficient and stable payments system, the Bank has been considering possible approaches to strengthening the handling of any future operational disruptions to ADIs' retail payments systems. Under section 10B of the *Reserve Bank Act 1959*, the Payments System Board has responsibility for determining the Bank's payments system policy so as to best contribute to:

- controlling risk in the financial system
- promoting the efficiency of the payment system
- promoting competition in the market for payment services, consistent with the overall stability of the financial system.

In addressing retail payments systems resilience, the Bank is conscious of the need to coordinate with the Australian Prudential Regulatory Authority (APRA) and the Australian Payments Clearing Association (APCA) so as to avoid duplication.

APRA is the prudential supervisor of the Australian financial services industry. As part of this role, APRA currently imposes a Prudential Standard on all APRA-regulated institutions, including ADIs, concerning business continuity management.[2] The standard takes a 'whole-of-business' approach and sets minimum high level requirements. However, it does not, nor is it intended to, set specific requirements concerning operational resilience standards for retail payments systems.

APCA is a self-regulatory body for the payments industry. It is responsible for developing and managing regulations, procedures, policies and standards governing the clearing and settlement of various types of payments, as well as facilitating communication and coordinating strategic initiatives between industry members.

2 The relevant Prudential Standard (CPS 232) is available at <http://www.apra.gov.au/adi/PrudentialFramework/Pages/prudential-standards-and-guidance-notes-for-adis.aspx>.

3. Informal Consultation

During the informal consultation process the Reserve Bank met with 15 interested parties. These included APRA, APCA, all four of the major banks, as well as a number of representatives of smaller ADIs, third-party service providers and technology providers. Discussions spanned a range of topics, including sources of vulnerability, safeguards and contingencies, and plans for upgrade and enhancement of supporting technology.

In general, the Bank observed an encouraging level of industry attention on operational resilience, with a number of payments system participants citing commercial pressures as a driver of increased investment in payments infrastructure. Moreover, payments operations are increasingly perceived as a strategic priority within financial institutions.

The following sections summarise the key learnings from the informal consultation process, covering the drivers for change within the industry, approaches to change management, business continuity arrangements, outsourcing and offshoring risks, and incident monitoring and communication arrangements.

Drivers for Change

Reputational pressure

Prominent operational incidents in retail payments systems attract considerable negative publicity, which may have adverse reputational implications for any ADI experiencing a difficulty. Given the number of prominent incidents that have occurred in recent years, customers are particularly sensitive to the associated disruption. Even though the ADI responsible for a problem does not bear the full cost of its disruption, the consequent reputational damage may be a sufficiently strong commercial driver for improvements in operational resilience.

Legacy systems

A concern prevalent among many payments system participants is the operational risk that arises from the continued use of legacy systems. The informal consultation confirmed the Bank's understanding that until recently many participants have tended to underinvest in payments infrastructure. As a result, there is widespread reliance on ageing core payments systems characterised by complexity and excessive interdependence between components. Such investment has been resisted due to the substantial cost of generational change, as well as the difficulty in upgrading systems essential to day-to-day operations while minimising interruptions to critical services.

Adding to this complexity are layers of modifications, which have been introduced incrementally over many years on an ad hoc basis. Given these characteristics, legacy systems may react unpredictably in response to new changes, which can lead to instability. Furthermore, the continued use of legacy systems entails a reliance on related skills, including in certain ageing programming languages, which are becoming increasingly

difficult to source. Key person risks are consequently becoming more concentrated as skilled workers leave the workforce, while new entrants are not qualified in such legacy skills. Some institutions mitigate this issue with the use of legacy skill training programs, though many recognise that widespread system upgrades will be the only solution in the long term.

Consumer demand

Another common theme arising from the consultation was the significant pace at which consumer demands for payment services are evolving, and the increased pressure this places on operational resilience. Consumer demands for a range of new capabilities have grown strongly, most notably around faster payments and mobile payments. However, due to the inflexibility of legacy systems, financial institutions have found it difficult to adapt to meet changing consumer expectations with their current payments infrastructure. As a consequence, the payments industry has been increasingly cognisant of the benefits of generational upgrades.

Strategic Review of Innovation

Payments system architecture was also considered as part of the Bank's *Strategic Review of Innovation in the Payments System*. As a result of this review, the Payments System Board is taking a more proactive role in setting strategic objectives for the payments system. In June, the Board proposed the following initial strategic objectives:[3]

- All Direct Entry payments should be settled on the day payment instructions are exchanged by the end of 2013.
- There should be the capacity for businesses and consumers to make payments in real time, with close to immediate funds availability to the recipient, by the end of 2016.
- There should be the ability to make and receive low-value payments outside normal banking hours by the end of 2016.[4]
- Businesses and consumers should have the capacity to send more complete remittance information with payments by the end of 2016.
- A system for more easily addressing retail payments to any recipient should be available.

Achieving any of these objectives will require changes to payments system participants' retail payments operating systems.

Change Management

For the reasons outlined above, financial institutions increasingly recognise a business case for transformative change in payments infrastructure. Accordingly, substantial investment is currently underway across the largest payments system participants. Many investment plans extend several years into the future and are often an important element of broader corporate strategy.

As upgrade programs are undertaken, the payments industry has initially seen an increasing incidence of disruptions, in part stemming from the upgrade process. Reflecting this, during the informal consultation a

3 RBA (2012), *Strategic Review of Innovation in the Payments System: Conclusions*, June. Available at <http://www.rba.gov.au/payments-system/reforms/strategic-review-innovation/conclusions/index.html>.

4 In November, the Board amended this strategic objective to omit out-of-hours capability for the Direct Entry system. It will review this when a fast payments solution is operational.

number of institutions stressed the importance of effective change management. In addressing this issue, many industry participants now proactively set strategies for payments operations and standardise frameworks to govern the change process. Relatedly, many institutions have established a central body for administering payments strategy. Typically, these bodies serve as an information-sharing hub, though their particular mandates vary across institutions. Payments system participants also generally share a belief in institution-wide governance of payments operations, as well as clear accountability and strong management controls. While many payments system participants implement changes on a quarterly or similar schedule, others advocated more frequent, incremental updates to ensure familiarity with the change management process.

Business Continuity Arrangements

Payments system participants unanimously emphasised the importance of sound business continuity management. A common strategy employed by the industry is the use of layers of redundancy in institutions' infrastructure, often distributed across primary and backup sites; this may be applied to core payments operations, including key personnel, as well as support functions such as monitoring and communications. The use of geographically diverse operating sites mitigates an institution's vulnerability to location-specific shocks. Relatedly, many institutions also employ 'follow-the-sun' IT support using personnel distributed globally across time zones.

The most reliable – and costly – form of this strategy involves duplicate systems operated independently, but in parallel, on an 'active-active' basis. In this case, the workload is spread across multiple versions of the system, although each is individually capable of managing the entire load if necessary. Under such an arrangement, if one component fails, transactions automatically fail over to another component. However, some respondents noted that technological limitations currently restrict the use of active-active arrangements for databases. Instead, redundancy arrangements usually involve synchronised replication of transaction records in both the primary and backup versions of a database.

Outsourcing and Offshoring

Outsourcing is generally recognised as a potential source of vulnerability. The degree of reliance on outsourcing arrangements varies significantly among payments system participants. The most commonly outsourced functions include IT support and systems software. Institutions stressed the importance of contractual terms to ensure reliable service provision, with key performance indicators often included in Service Level Agreements. To mitigate the risk associated with outsourcing, some institutions insist that third-party providers allocate dedicated personnel, in some cases further requiring that these personnel co-locate at the payments system participant's premises. In addition, institutions typically hold regular review meetings with each third-party provider as a means of monitoring service levels. The Bank noted some dependencies on common third-party providers across a number of institutions, which could be viewed as a potential common source of vulnerability to payments system participants.

Another related practice is the use of offshoring. Offshoring is defined as the outsourcing of services to an entity (including to a related corporate body) that conducts the outsourced activity outside of Australia. Although governance arrangements for offshoring may be stronger than those for standard outsourcing, offshoring may nevertheless add to potential operational risks stemming from dislocation of activities. Time zone differences may exacerbate these issues. On the other hand, offshoring may also make it easier to provide 24/7 operational support, thereby potentially enhancing resilience.

Incident Monitoring

Most institutions conduct real-time monitoring of their own operating systems to quickly identify and escalate any issues, with some institutions supplementing this with third-party monitoring services. The larger financial institutions conduct monitoring on a 24/7 basis and tend to favour highly automated, centralised arrangements for monitoring internal processes. Some have invested considerably in recent years to enhance their monitoring capabilities.

It was noted that monitoring the end-to-end process for each payment instrument (i.e. from the initiation of a payment by a customer through to final settlement), rather than discrete systems or functions is likely to provide a clearer view of the customer's experience in using that payment instrument. Monitoring processes are therefore typically designed accordingly. In terms of managing operational performance and escalation procedures, a number of institutions have revised their incident severity classifications and performance metrics to better reflect the business and customer impact of incidents.

Communications

A number of industry participants identified the potential to improve communications within the industry (i.e. between payments system participants) and between payments system participants and their customers, both during and following significant incidents. In particular, it was observed that the dissemination of information does not always occur in a timely manner, and sufficient details are not routinely provided.

4. The Reserve Bank's Response

The Reserve Bank is taking a number of actions in response to retail operational incidents. These include formalising its incident reporting arrangements, strengthening its understanding of individual participants' payments infrastructure, and introducing regular statistical reporting. These actions reflect the Bank's desire to ensure that operational resilience remains a strategic priority among payments system participants.

Incident Reporting

In February 2012, the Bank extended its formal incident reporting requirements for high-value payments to cover significant incidents in retail payments systems.[5] Leveraging existing reporting arrangements, these new requirements apply to all members of the Reserve Bank Information and Transfer System (RITS). While not all retail payments system participants are RITS members, and therefore subject to these reporting requirements, the majority of retail payments are processed through RITS members.[6] An alternative approach would be to use the Bank's powers under section 26 of the *Payment Systems (Regulation) Act 1998* to require payments system participants to provide information relating to payments systems. This is a broad power that could be used to collect information from all payments system participants. If the Bank forms the view that the current scope of the reporting arrangements is providing insufficient information, this alternative approach could be pursued.

Under current arrangements, RITS members are required to report to the Bank any incidents that have a significant impact on retail payments. The Bank has defined reportable incidents according to their effect on customers' access to particular payments channels or account information, the impact on clearing or settlement activity, the use of business continuity arrangements, or media coverage (see Box A for details of the criteria). RITS members are required to notify the Bank within one hour of any reportable retail incident, with further updates to be provided at least every two hours for the duration of the incident. In doing so, RITS members are required to provide information on the probable cause, customer impact, systems impacted and recovery strategy, as well as the expected recovery time frame and likely impact on other financial institutions.

The Bank has invited feedback from participants on the reporting criteria and, going forward, will refine these as appropriate. During the informal consultation, some members requested clarification on the applicability of specific criteria and time frames for reporting of incidents occurring overnight; these matters will be considered when the criteria are refined.

The Bank also requires RITS members to provide detailed post-incident reports for each reportable retail incident. The post-incident report must explicitly cover the time line of the incident, the incident's root

5 The Incident Reporting requirements are specified at <http://www.rba.gov.au/payments-system/rits/user-doc/pdf/incident-reporting-arrangements.pdf>.

6 A list of current RITS members is available at <http://www.rba.gov.au/payments-system/rits/membership/membership-list.html>.

cause and impact, as well as the management of the incident and proposed remedial actions. The Bank has developed an optional incident reporting template to assist RITS members in meeting this requirement.

To ensure compliance with the reporting criteria, the Bank plans to engage bilaterally with all RITS members with significant retail payments operations to ensure their familiarity with the requirements and to ensure that these are included in their incident management procedures. Feedback on the criteria will also be sought at that time.

Box A
Reportable Retail Incidents

Customer Access

1. ATM or point-of-sale payment stream (e.g. EFTPOS, credit/debit cards) is unavailable or incorrectly rejecting transactions (card, transaction or balance checking) across a major geographical area (e.g. a city CBD, regional area, or multiple suburbs) for a period of one hour or more.
2. Disruption to any other customer interface (e.g. online banking, telephone banking, mobile applications, direct links or portals) that:
   (a) potentially affects more than 100 000 customers or 25 per cent of the institution's customer base (whichever is lower); or
   (b) lasts for more than two hours.

Account Maintenance

1. More than 250 000 accounts or 25 per cent of the institution's customer accounts (whichever is lower) not being correctly updated, as follows:
   (a) delays in posting to accounts past usual times;
   (b) duplicated or missing transactions; or
   (c) funds not available to customers within normal time frames.

Clearing Activity

1. Missing (or delaying by over two hours) more than one scheduled APCA clearing system file exchange with one or more institution.
2. Missing defined BPAY cut-off times.
3. The clearing of card-based transactions (e.g. EFTPOS, debit/credit cards) with one or more other institution is unavailable for a period of one hour or more (excluding scheduled maintenance activities).
4. Use of alternative transmission means, such as encrypted email.
5. Other material disruption to clearing operations, including but not limited to duplicate or rejected file exchanges.

Settlement Activity

1. Inability to send settlement instructions to RITS for low-value clearings with other institutions, or use of contingency facilities to submit these instructions.

Operating Site

1. Any need to invoke business continuity or disaster recovery arrangements requiring recourse to one or more key systems at an alternative site.

Media Coverage

1. Where a retail payments system problem receives substantial media coverage (e.g. is reported in the online version of a national newspaper or on a television news program website).

Systems Descriptions

To facilitate the Bank's ability to assess the incident reports it receives, the Bank is collecting high level information from RITS members regarding their payments infrastructure. This information will cover data centre arrangements, a description of each critical system used to deliver payment services to customers, as well as process flows for a selection of critical systems used for the provision of retail payment services. It is expected that these systems descriptions will be updated on a periodic basis to ensure the information remains sufficiently current.

Statistical Reporting

The Bank foreshadowed in the RITS Advice announcing the incident reporting protocol that it would also introduce regular statistical reporting on retail payments incidents. The Bank noted that it would consult with RITS members on the scope and format of this reporting. The Bank has prepared a draft reporting template on which it will be seeking feedback from RITS members. While the coverage of incidents will be broader than that encompassed by the incident reporting arrangements, the focus will be on trends rather than individual incidents (see Box B for details). It may also be the case that an increase in the occurrence of minor incidents is a leading indicator of more severe problems.

It is expected that the statistics will cover the frequency of incidents by severity, duration, payments channel, time of commencement and root cause. These statistics are aimed at identifying sources of vulnerability and measuring the impact on customers. For example, incidents that affect point-of-sale payments channels during business hours are likely to cause more disruption to customers than internet banking outages in the middle of the night.

As with the incident reporting protocol, the Bank could collect these statistics using its powers under the Payment Systems (Regulation) Act. It may choose to do so if it establishes that a material proportion of retail operational incidents occur in systems operated by participants that are not RITS members.

Box B
Severity Criteria

RITS members will be required to provide summary statistics on retail payments incidents that fall into one of three severity classes specified in Table 1, which are defined according to the same parameters as those used to define reportable incidents. Where an incident meets more than one set of criteria, the highest severity level will be reported.

Table 1: Severity Level Criteria

	Severity 1	Severity 2	Severity 3
Customer access	All reportable incidents (see Box A)	ATM/EFTPOS: 30 min–1 hr Other: 15–25% or 60 000–100 000 customers; or 1–2 hrs	ATM/EFTPOS: 15–30 min Other: 5–15% or 20 000–60 000 customers; or 30 min–1 hr
Account maintenance		15–25% or 150 000–250 000 accounts	5–10% or 50 000–100 000 accounts
Clearing activity		Cards: 30 min–1 hr Other APCA: 1–2 hrs	Cards: 15–30 min Other APCA: 30 min–1 hr
Settlement activity		n/a	n/a
Operating site		n/a	n/a
Media coverage		Only reported online or in a state newspaper	n/a

5. Additional Measures

The consultation process has helped to further develop the Bank's views on alternative measures to enhance ADIs' retail operational resilience. In February 2012, the Payments System Board reviewed options to supplement the reporting requirements with additional measures, including enhanced disclosure, improved communication arrangements and retail resilience standards. While there may be merit in some form of resilience standards, in light of the progress already being made by industry, the Bank plans at least for the time being to limit its role to monitoring retail operational incidents and working with industry on initiatives around disclosure of data on incidents.

Monitoring and Disclosure

The Bank will maintain an ongoing role in monitoring and analysing data from RITS members' incident reporting and the regular statistical reporting. In cases where the Bank believes that a particular payments system participant is persistently underperforming, or that the remedial measures it implements are inadequate, the Bank intends to follow up with the participant. In such scenarios, the Bank would initiate high-level meetings with the participant's management. It is likely that APRA would also be involved. More generally, it is expected that key information on operational incidents provided to the Bank would be made available to APRA to assist in its oversight of the institutions involved.

In addition, the Bank will be discussing with APCA options for disclosing the aggregate statistical data on operational incidents. Aggregate data could potentially be published to provide the public with reliable information on the prevalence of retail operational incidents. Alternatively, disclosure of aggregate data could be limited to payments system participants, who could use these data for performance benchmarking purposes. The Bank strongly encourages such benchmarking, and will work with the industry in achieving such an outcome. Ultimately, enhanced disclosure would be expected to maintain the momentum behind ongoing efforts to improve operational resilience, and ensure that institutions' senior management remain engaged on this issue.

Communication

Prior to the Bank's informal consultation, APCA had already identified the need to improve industry communications in the event of an operational incident. To address this, APCA has implemented an enhanced incident management process, which involves three levels of escalation. APCA is refining the routine 'processing difficulty notifications' that members use to advise other APCA members of any operational issues they are experiencing, including by adding the option to provide updates on an incident. APCA has also developed a Member Incident Plan, which if invoked would trigger conference calls between members during significant

incidents. Under the enhanced incident management process the Management Committee of the relevant clearing stream has the option of escalating the incident to APCA's Crisis Management Team, which would activate its crisis communication plan. Together, these initiatives are designed to centralise and streamline industry communications. The Bank is supportive of this work.

In addition, the Bank sees potential benefits in the industry conducting 'post-mortems' of significant incidents in the future. Such investigations would be designed to increase understanding of common vulnerabilities between payments system participants' operations and improve incident management best practice in the industry.

Retail Resilience Standards

Neither APCA nor APRA currently sets operational resilience standards specifically in respect of retail payments. APRA does, however, set business continuity expectations that apply to ADIs' critical business functions generally. APCA requires its members to establish and test contingency arrangements for exchanging payment instructions with other members (e.g. via email), but currently imposes no requirements in respect of customer interfaces.

The Bank is currently consulting with RITS members on draft business continuity standards for RITS, which aim to promote 'high availability' where processing of RITS payments is concerned, requiring both resilience of system components and rapid recovery if failover to alternative systems is required. These standards cover business continuity planning, system resilience, incident management, recovery time frames and business continuity testing. To the extent that RITS members manage their payments operations holistically, improvements in best practice for high-value payments may flow on to retail operations.

There could be some benefit to the payments industry from some form of resilience standards for retail payments systems. In principle, these could be voluntary standards developed by industry, contractual requirements imposed on RITS members, or standards set by regulators. The purpose of such standards would be to improve the resilience of retail payments systems by increasing payments system participants' focus on, and resourcing of, their retail payments operations, or through identifying and addressing information asymmetries that may be limiting participants' ability to improve their operational resilience.

While the Bank would, in principle, be supportive if the industry developed such standards, the Bank does not see a case at this stage for developing or implementing such standards itself. The informal consultation highlighted that individual participants are aware of the issues and are actively working towards improving the resilience of their systems. Given that the resilience of retail payments systems is already a high-profile issue within the payments industry, it is not clear that introducing retail resilience standards at this time would increase payments system participants' focus on this issue. However, if in implementing the other measures set out in this paper, the Bank identified a potential need to impose such standards, it would review this decision.

6. Conclusions

The Reserve Bank has completed an informal consultation on retail operational incidents. During this process, the Bank met with 15 interested parties, including all four of the major banks. In general, the Bank observed an encouraging level of industry attention on operational resilience, with a number of payments system participants citing commercial pressures as a driver of increased investment in payments infrastructure. Moreover, payments operations are increasingly perceived as a strategic priority within financial institutions.

As a result of the informal consultation, the Board has concluded that at present there is no need for a regulatory response. Indeed, in the Board's view, senior management of individual institutions are primarily responsible for improving the operational resilience of their organisations. Accordingly, the Bank plans at least for the time being to limit its role to monitoring retail operational incidents and working with industry on initiatives around the disclosure of data on incidents.

Consistent with this, the Bank has implemented an incident reporting protocol and is in dialogue with RITS members on the collection of additional information on the system architecture supporting retail payments activities, as well as a framework for routine statistical reporting on retail payments incidents. The data collected under this reporting framework would be used to identify trends and follow up with any payments system participant that was persistently underperforming. The data could also form the basis for industry initiatives to disclose aggregate data on operational incidents to facilitate performance benchmarking by payments system participants.

The Bank's involvement in matters related to retail payments system resilience is likely to evolve over time. The Bank therefore plans to maintain an open dialogue with the industry. Moreover, the Bank will continue to refine its incident reporting requirements and other information-gathering activities. In due course, the analysis of information obtained from these sources will provide sound evidence as to whether further action is necessary.