RTGS AND RETAIL PAYMENTS INCIDENT REPORTING ARRANGEMENTS FOR RITS MEMBERS

DATE OF ISSUE: 30 AUGUST 2017

1. Overview of Incident Reporting Arrangements

The incident reporting arrangements detailed in this document apply to RITS Members that settle RTGS transactions and/or retail payments (including NPP).

The incident reporting arrangements consist of the following parts:

- Reporting of incidents affecting settlement across RITS of RTGS and other payments
- Reporting of incidents affecting retail payments systems
- Reporting of incidences of successful or partly successful cyber-attacks
- Provision of statistical information on retail payments outages.

The table below summarises the main aspects of incident reporting by Members. Detailed requirements are then set out in the following sections.

	Settlement in RITS (including 'high value' RTGS transactions)	**Retail payments including NPP ('low value' transactions)**
Systems affected	Core payment application; SWIFT CBT; AML; RITS access; internal and external networks	All systems that are involved in processing of retail payments. Included in the scope are: ATMs (including cardless access), EFTPOS, cheque clearing, direct entry and BPay payments, credit, debit and prepaid cards transactions (as acquirer or issuer), as well as all customer interfaces such as telephone banking, internet banking, mobile banking and social media banking.
Reportable incidents	Incidents preventing efficient settlement of payments in RITS	Incidents with a significant impact on retail payments

	Settlement in RITS (including 'high value' RTGS transactions)	Retail payments including NPP ('low value' transactions)
Initial notification to RITS Help Desk	Immediately the incident becomes apparent	Within one hour of the incident becoming apparent, or within 30 minutes for NPP-related incidents.
Incident updates	Every 30 minutes	Every one to two hours, or every 30 to 60 minutes for NPP-related incidents.
Written incident reports	Where normal settlement activity is interrupted for a period of 30 minutes or more, a report is to be submitted within one week. If this is an interim report, the final report is normally required within four weeks.	Where an incident meets the criteria in section 2.2, a report is to be submitted within one week. If this is an interim report, the final report is normally required within four weeks.

2. REPORTABLE INCIDENTS

RITS Members are required to contact the RITS Help Desk to advise that an incident has occurred if it meets the criteria for reportable incidents as set out below.

2.1 All payments – RTGS and other payments

Members are to immediately report to the Reserve Bank all operational incidents that prevent efficient settlement across RITS of RTGS and other payments.

Members must contact the RITS Help Desk on 1800 659 360 as soon as a problem becomes apparent. Members are reminded of their responsibility to ensure effective monitoring during the RITS operational day of their ESA and transactions submitted to RITS for settlement. Members should be particularly vigilant after any upgrades or other changes are made to their internal systems.

The Australian Payments Network Limited's (AusPayNet, previously APCA) High Value Clearing System (HVCS) Procedures require that Participating Members advise the System Administrator (the Reserve Bank) immediately upon becoming aware of any technical or operational problems with their SWIFT computer-based terminal (CBT) or in-house payment system that prevents them from processing SWIFT PDS payments. The HVCS Procedures reporting requirements are satisfied by reporting under the arrangements outlined in this Advice.

2.2 Retail payments

Members must report incidents affecting retail payments systems that meet any of the following criteria:

Settlement activity:

- Inability to send settlement instructions to RITS for low value clearings with other institutions i.e. missing a low value multilateral settlement run.

- For NPP transactions, the inability of a payer bank to send a settlement request to the Fast Settlement Service within 30 minutes of receiving a clearing notification from a payee bank.

Clearing activity:

- Missing (or delaying by over two hours) more than one scheduled APCA clearing system file exchange with one or more institutions.
- Missing defined BPAY cut-off times.
- The clearing of card-based transactions (e.g. EFTPOS, debit/credit cards) with one or more institutions is unavailable for a period of one hour or more (excluding scheduled maintenance activities).
- Use of alternate transmission means for clearing file exchange, such as PGP email.
- Other material disruption to clearing operations, including but not limited to duplicated or rejected file exchanges.
- For NPP transactions, when the payer bank is unable to send clearing requests for a period of 30 minutes or more after a payer initiates a payment through one of the bank channels (e.g. online banking, mobile banking, etc.).
- For NPP transactions, when the payee bank is unable to respond to a clearing request with a clearing notification for a period of 30 minutes or more.
- For NPP transactions, the inability by a payee bank to credit receiving customer accounts within 30 minutes after either a valid clearing message or positive settlement notification has been received (in accordance with applicable overlay requirements).

Operating site:

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

Customer access:

- ATM or point-of-sale payment stream (e.g. EFTPOS, credit/debit cards) is unavailable or incorrectly rejecting transactions across a major geographical area (for example, a city CBD, regional area, or multiple suburbs) for a period of one hour or more.
- ATM or point-of-sale payment stream (e.g. EFTPOS, credit/debit cards) reverts to stand-in mode (e.g. withdrawals or purchases capped to a floor limit or store and forward mode) across a major geographical area (for example, a city CBD, regional area, or multiple suburbs) for a period of one hour or more.
- Disruption to any other customer interface (e.g. online banking, telephone banking, mobile banking, mobile payments, cardless ATM withdrawals or social media banking) 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:

- 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.

Media coverage:

- Where a retail payment system problem receives substantial media coverage (e.g. is reported in the online version of a national newspaper or on TV news programme website).

2.3 Reporting of Cyber-Attacks

Due to the growing threat of cyber-attacks on financial institutions which can significantly disrupt services and undermine the integrity and resilience of RTGS and retail payments systems, the Reserve Bank requires Members to report successful or near-miss (i.e. partly successful) cyber-attacks on these systems.

Should a cyber-attack to RTGS and retail payments systems result in a reportable incident the reporting arrangements outlined in sections 2.1, 2.2 and 3 apply. The incident report should include the root cause of the cyber-attack and details on preventative actions that will be taken to avert, or minimise the impact of, such threats in the future.

Members are also requested to inform the Reserve Bank of instances of a cyber-attack that does not result in a system outage, but where there has been a breach of a Member's normal IT security controls.[1] The information, including details such as the root cause of the cyber-attack and preventative actions taken, should be provided to the Reserve Bank within two weeks of the incident, via a letter marked for the attention of the Head of Payments Settlements, and posted to the Reserve Bank or emailed to rits@rba.gov.au.

2.4 Reporting during Natural Disasters and Major Infrastructure Outages

Natural disasters and major outages of infrastructure such as telecommunications and electricity have the potential to disrupt RITS Member's payments activity in the affected area. In these cases, following the initial notification of the event to the RITS Help Desk, status updates from Members will suffice, instead of the reporting arrangements outlined in section 3.

Status updates should generally be provided daily, but may be more frequent if there are significant changes to a Member's operational status or provision of retail payments services. Once the recovery from the event is well underway, less frequent reporting may be appropriate. The Member may cease providing status updates when service restoration has been substantially completed.

The following information should be provided to the Reserve Bank:

- Business impacts (including access channels and payments products)

  Member status updates should include summary details of service outages (e.g. number of ATMs/EFTPOS terminals affected, number of branch closures or branches operating with limited services, impacts to online/phone/mobile banking and mobile payments, and other

[1] For instance, this would exclude attacks on the perimeter that are repelled by firewalls but would include the discovery of a Trojan that has gained a system foothold without causing an outage.

payment channels). Status updates may also include disruptions to other operations such as cheque clearing.

- Mitigations being applied whilst restoring services

  This may include any business continuity procedures invoked (e.g. mobile ATMs despatched, branch workarounds including capping the value of withdrawals, additional cash deliveries or EFTPOS terminals reverting to contingencies such as stand-in or store and forward mode.)

- Service restoration progress and anticipated restoration time

  Status updates should include the status of services being brought back online (e.g. number of ATMs now operational or number of branches providing wider service since previous status update), where possible with anticipated date or time to achieve full restoration.

3. Incident Management and Reporting

3.1 Initial Notification to the RITS Help Desk

As part of their incident management procedures, Members must notify the RITS Help Desk (1800 659 360) of any reportable incident: immediately for an RTGS operational incident; and within one hour for a retail payments operational incident. Members can contact the RITS Help Desk on a 24x7 basis.

The following information is required to be provided during an incident:

- Advise RBA of communication arrangements:
  - standard contact point for the duration of the issue
  - escalation point (confirm existing contact or advise another)
  - frequency of updates
  - means of update (via phone or email)
- The Member should provide information on:
  - possible cause
  - customer impact
  - systems impacted
  - recovery strategy
  - expected recovery timeframe

For prolonged outages an executive-level conference call may be initiated.

Updates must be provided at least every 30 minutes for RITS incidents and every 30 to 60 minutes for NPP-related incidents. For other retail payments incidents, updates should be made every 1 to 2 hours unless otherwise agreed with the Reserve Bank.

3.2 Post-Incident Reporting

Members must provide the Reserve Bank with a detailed post-incident report for any RITS incident that disrupts settlements for 30 minutes or more, or any retail payments operational incident that is reportable in terms of the criteria in section 2.2. The Reserve Bank also requires a written report in the event that a Member fails to bring its projected 9am ESA balance into credit by the close of the Morning Settlement Session at 8.45 am. The report, or an interim report if further investigation is required, must be received by the Reserve Bank within one week of the incident. Where an interim report is submitted, a final report should normally be submitted within four weeks of the incident.

The report should address the following:

- Outline of incident, with accompanying timeline (including key decision points and actions)
- Root cause
- Internal system impact
- Business impact
- Impact on other institutions
- How the problem was detected
- Decision making process regarding recovery of systems
- Mitigating actions put in place while the problem was resolved
- How the problem was rectified
- Were internal incident management procedures followed
- Were internal communications protocols applied and used effectively
- Handling of external communications, i.e. with other banks, customers, vendors
- Proposed actions to prevent recurrence or mitigate its impact, and targeted timeframe for completion

The report should be marked for the attention of the Head of Payments Settlements, and posted to the Reserve Bank or emailed to rits@rba.gov.au. The incident report will be reviewed and a formal response provided by the Reserve Bank. Reports provided to the Reserve Bank may be copied by the Member to AusPayNet or APRA at the Member's discretion. The Reserve Bank may discuss incidents with APRA.

The Reserve Bank has a template Incident Report that Members may use for their interim and final reporting (attached).

3.3 Service Provider Incident Reporting on Behalf of Members

Where a Member uses a service provider to deliver retail payment (e.g. clearing and settlement) or other services (e.g. utilities), and a reportable incident has occurred, the Member may provide to the RBA, incident reports supplied to them by their service providers, as long as the informational requirements set out in the reporting arrangements are met.

3.4 Provision of Statistical Information on Retail Payment Outages

The Reserve Bank requires Members that offer retail payment services to provide statistical information on incidents affecting those services on a quarterly basis. The Reserve Bank's Statistical Collection Form should be used. The Reserve Bank sends the Statistical Collection Form to relevant RITS Members quarterly, as part of the reminder email that the statistical information is due.

Members are required to provide statistical information on all retail payments outages, not just those that meet the reporting criteria in section 2.2 of this document. For the statistical information, incidents that are reportable under the criteria in section 2.2 of this document are referred to as 'severity 1'. Other incidents affecting retail payments are referred to as 'severity 2'.

Anonymised aggregate summary information from this statistical collection is provided to AusPayNet to make available to reporting Members who may wish to use this summary information for benchmarking purposes.

3.5 Member Systems Descriptions Reporting

The Reserve Bank has previously requested Members to provide information on their retail and high-value payment systems, including corresponding process flows, and information on primary and secondary data centres to assist the Reserve Bank in its review of Member incident reports.

Members should update the information provided in their Systems Description reports when significant changes are made to their critical payment systems.

INCIDENT REPORT

Please send completed reports to:

To: Head of Payments Settlements

Email: rits@rba.gov.au.

Fax: +612 9551 8063

Post: Head of Payments Settlements
Reserve Bank of Australia
GPO Box 3947
SYDNEY NSW 2000

Should Members elect to send documentation via encrypted email, please provide details for the Reserve Bank to obtain the encryption code.

Respondent Details:

Organisation:

Contact Name:

Contact Phone:

Contact Email:

Report Status	**Date**
Incident Report **Interim** or **Final** (please delete as appropriate)	

Authorised By:

.....
(name)

.....
(signature)

Where applicable, please attach your Major Incident Review or other accompanying incident documentation.

INCIDENT REPORT

INCIDENT DETAILS	RESPONSES
Date of incident	
Incident description & root cause	
Incident start time	
Incident end time	
Duration of service(s) outage[2]	
Internal system(s) (e.g. hardware, software or network) & function(s) (e.g. processing) impacted	
Business Impacts – RTGS or retail payments products & channels affected	
How the incident was detected	
What decisions were made leading to recovery of systems	
What mitigations were applied whilst resolving the incident	
How was the problem rectified	
How appropriate were internal incident management procedures & communications	
Were other institutions impacted	
External Communications - how were customers, banks & vendors notified	
What future action items to prevent reoccurrence have been agreed to & by when	

[2] Times between incident and outage may differ (e.g. change failure lasting 300mins yet EFTPOS outage lasting 185mins).

INCIDENT REPORT

INCIDENT TIMELINE		
Date	**Time**	**Incident Event Sequence (Include Events, Decision Points, Actions & Outcomes)**