RITS MEMBER INCIDENT REPORTING ARRANGEMENTS

DATE OF ISSUE: 3 SEPTEMBER 2024

1. OVERVIEW

The incident reporting arrangements detailed in this document apply to RITS Members that operate an Exchange Settlement Account (ESA) with the Reserve Bank, or are batch administrators submitting batches in RITS for the settlement of card, equities or property settlement transactions. These reporting requirements do not apply to 'dormant' ESA holders that settle all of their RTGS transactions via an RTGS agent, or 'non-transactional' RITS Members that do not hold an ESA nor are a batch administrator.

These incident reporting arrangements address reporting of incidents that:

- affect settlement across RITS of wholesale RTGS payments, including file submission by external batch administrators
- affect retail payments systems that impact RITS operations
- involve successful or partly successful cyber-attacks on RTGS or retail payments systems.

The arrangements also clarify:

- the handling of incidents that involve system-wide infrastructure outages and natural disasters
- reporting requirements when utilising service providers (where the incident is not a system-wide outage or natural disaster).

These arrangements are in addition to requirements for certain RITS Members to provide quarterly reporting of statistical information on retail payments incidents, which are documented separately.[1]

[1] The Reserve Bank requires certain RITS Members offering retail payment services to provide statistical information on incidents affecting those services on a quarterly basis. It also requires around 30 individual institutions providing retail payment and banking services to end customers to publicly disclose a standard set of quarterly statistics on service outages and availability.

The table below summarises the differences between reporting of 'wholesale' and 'retail' incidents. Detailed requirements are set out in the following sections.

	Wholesale payments (including 'high value' RTGS transactions and externally administered batch files)	**Retail payments (including NPP and other 'low value' transactions)**
Systems affected	Core payment application; SWIFT CBT; AML; sanctions screening; RITS access; internal and external networks.	All systems that have the potential to impact RITS operations, including systems that process clearing files and submit settlement instructions.
Clearing and settlement arrangements affected	SWIFT PDS; Austraclear; RITS cash transfers; file submission by external batch administrators (ASXF, CHESS, EFTPOS, Mastercard, and PEXA).	NPP; IAC; APCS; BECS; LVCS; LVSS
Reportable incidents	Incidents preventing efficient settlement of payments in RITS. Any wholesale payments incident requiring the use of back-up and contingency services, including those at alternate sites.	Incidents with an impact on RITS operations, including those impacting clearing activities and the ability to submit settlement instructions to RITS, including FSS. Any retail payments incident requiring the use of back-up and contingency services, including those at alternate sites. Any retail incident where the Reserve Bank specifically requests updates or an incident report, which it may do for retail incidents with significant customer impact.
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 hour, unless otherwise agreed with the RITS Help Desk.
Written incident reports	A post-incident report is required: • Where normal settlement activity is interrupted for a period of 30 minutes or more. • Where there is a material delay to submission of a batch request file by an external batch administrator. • Where there is a material delay by a batch participant to making funds available to settle an external batch. • For all reportable cyber incidents meeting the criteria in section 2.3. • Where the Member fails to bring its projected 9am ESA balance into credit by the close of the Morning Settlement Session at 8.45 am.	A post-incident report is required: • If the incident meets the criteria in section 2.2. • For all reportable cyber incidents meeting the criteria in section 2.3. The report should be submitted within one week. If this is an interim report, the final report is normally required within four weeks.

	Wholesale payments (including 'high value' RTGS transactions and externally administered batch files)	Retail payments (including NPP and other 'low value' transactions)
	The report should be submitted within one week. If this is an interim report, the final report is normally required within four weeks.	

For the purposes of incident reports relating to externally administered batch files, the criteria for a 'material delay' depends on factors such as the type of batch, the time of day that the batch would normally be submitted, and whether the incident involves funding and/or batch submission, and are agreed between the Reserve Bank and the batch administrator.[2]

As a general guide, a delay of more than around one (1) hour from the usual submission time (or where there are multiple submissions per day, a delay of more than around 1 hour after the final submission of the day) would be considered 'material'.

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 Wholesale Payments

Members are to immediately report to the Reserve Bank all operational incidents that prevent efficient settlement of wholesale payments across RITS. This includes settlement of SWIFT PDS, Austraclear, and RITS cash transfer transactions. External batch administrators are required to report all operational incidents where there is a material delay to the submission of a batch request file. Batch participants may also be required to report an incident where there is a material delay to their making funds available to settle a batch. An incident where the Member fails to bring its projected 9am ESA balance into credit by the close of the Morning Settlement Session at 8.45 am is also a reportable incident. Although related to retail payments settlement, these last three incident types are treated as a 'wholesale' incident to reflect the scope of their impact. Members must also report any wholesale payments incident requiring the use of back-up and contingency services, including those at alternate sites.

Members must contact the RITS Help Desk on 1800 659 360 or +61 2 9551 8930 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 upgrades or other changes are made to their internal systems.

The Australian Payments Network Limited's (AusPayNet's) 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

[2] These criteria will be detailed in the Operational and Contingency Procedures for each respective Batch Administrator.

processing SWIFT PDS payments. The HVCS Procedures reporting requirements are satisfied by reporting under the arrangements outlined in this document.

2.2 Retail Payments

Members must report incidents affecting retail payments systems that impact RITS operations, including those impacting clearing activities and the ability to submit settlement instructions to RITS, including FSS. Members must also report any retail payments incident requiring the use of back-up and contingency services, including those at alternate sites.

Members must contact the RITS Help Desk on 1800 659 360 or +61 2 9551 8930 to provide initial notification within one hour of the incident becoming apparent, or within 30 minutes for NPP-related incidents. For NPP transactions, the incident is only reportable if it applies to more than 10 per cent of the total number of transactions being processed.[3]

The Reserve Bank may also specifically request information, including status updates and a post-incident report, for any retail incident of concern to the Bank, which would typically be any incident with significant customer impacts. This could, for example, include a major outage of card processing systems impacting merchants and retail customers, or an outage attracting significant media attention.

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 settlement requests to the FSS within 30 minutes of receiving clearing notifications from a payee bank for more than 10 per cent of the total number of transactions that were expected to be processed during the incident.

Clearing activity:

- Missing (or delaying by over two hours) a scheduled AusPayNet clearing system file exchange with one or more institutions. For BECS, an incident becomes reportable when more than one scheduled exchange is missed.
- Missing defined BPAY cut-off times.
- 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, if they have potential flow-on effects to RITS operations.
- For NPP transactions, when the payer bank, for more than 10 per cent of the number of transactions being processed, 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.).

[3] This is consistent with the threshold in the requirements for reporting of quarterly retail payment incident statistics to the Reserve Bank.

- For NPP transactions, when the payee bank is unable to respond to clearing requests with a clearing notification for more than 10 per cent of the number of transactions being processed over a period of 30 minutes or more.

Operating site:

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

2.3 Reporting of Cyber-Attacks

Cyber-attacks on financial institutions have the potential to significantly disrupt services and undermine the integrity and resilience of wholesale and retail payments systems. Therefore, successful or near-miss (i.e. partly successful) cyber-attacks on these systems are also considered to be reportable incidents. A near-miss includes a cyber-attack that does not disrupt normal payment operations, but where there has been a breach of a Member's normal IT security controls.[4]

For cyber-attack incidents, as for other incidents, Members must contact the RITS Help Desk to provide initial notification of the incident. The timing of initial notification and incident updates is as for other incidents, depending on whether the attack was directed at wholesale or retail payment systems. For example, a successful or near-miss cyber-attack targeting wholesale payment systems should be notified as soon as the problem becomes apparent, with updates to be provided every 30 minutes.

A post-incident report for these cyber-attacks is also expected, using the same format as for other incidents. This is required for both successful and near-miss attacks meeting the criteria in this section, regardless of their resulting impact on payment operations.

2.4 Reporting during System-wide Infrastructure Outages and Natural Disasters

System-wide infrastructure outages and natural disasters have the potential to disrupt RITS Members' payments activity in the affected area. System-wide infrastructure includes RITS and FSS, COIN, SWIFT, NPPA infrastructure (e.g. PayID), card scheme infrastructure, electricity networks, and telecommunication network links to the Member's data centres.

In these cases, following the initial notification of the event to the RITS Help Desk, status updates from Members will suffice. A post-incident report, as described in section 3, is not required.

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 in the status updates:

- 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

[4] 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.

limited services, impacts to online/phone/mobile banking and mobile payments, and other 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.

2.5 Incident Reporting involving Service Providers

This section defines arrangements for reportable incidents where the source of the problem is related to infrastructure of another entity that is providing payments processing services, but excluding system-wide infrastructure as defined above. In these cases, the ultimate responsibility for ensuring that initial notification, status updates and a post-incident report are made to the RITS Help Desk lies with the Member using the service provider. However, in cases where the incident is due to services that are provided by another active ESA holder, the service provider may for practical purposes provide reporting on behalf of the principal Member. This is on the basis that the service provider in these cases has both knowledge of the problem, and has a relationship with the RITS Help Desk with pre-defined contacts and escalation points, and is therefore best placed to provide timely and accurate reporting. This may, for example, apply in cases where an ESA holder is providing clearing and settlement agency services, or more specific message processing services.

Active ESA holders providing payments processing services for other RITS Members should note this means they are generally expected to provide the RITS operational incident reporting related to their operations (not the Member using the services). Where clearing and settlement agency services are being provided for transactions settled in RITS, the service provider should include in its post-incident report a description of how the incident has impacted the institutions that it is providing clearing and settlement services for, including the impacted institutions and clearing and settlement activities.

Where the service provider being used is not an active RITS Member (e.g. a generic IT infrastructure provider), the Member using the service is responsible for incident reporting and liaising with their service provider as required. If a post-incident report is required, the Member should provide the report in the required Incident Report Template, but may also submit incident reports supplied by their service providers for additional information.

2.6 Reporting of Incidents Related to Externally Administered Batches

Externally administered batches include settlement batches, used for daily net settlement of obligations arising from card and equities transactions, and reservation batches used for electronic property settlements. In cases where there is a material delay with the Batch Administrator's submission of the batch request file, or other issues related to administration of

the batch with impacts on RITS operations, the Batch Administrator is responsible for reporting the incident.

If, however, the batch request has been successfully submitted and settlement of the batch is delayed by a Member not having funds available to settle the batch (or otherwise delaying the batch settlement instruction as a result of their ESA settings), then both the Member and the batch administrator have some incident reporting responsibilities. The Member is responsible for initial notification of why they cannot make funds available to settle the batch and, if this is considered a reportable incident by the RITS Help Desk, is also responsible for the post-incident report. Batch administrators also have a responsibility to monitor batch status and are expected to notify the RITS Help Desk of delays to settlement, but would not be required to submit a post-incident report given that the issue lies with the batch participant.

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 by phone of any reportable incident: immediately for wholesale payments; and within one hour of incident becoming apparent for a retail payments operational incident (or 30 minutes for NPP-related incidents). These same requirements also apply in the case of cyber-attack incidents, depending on whether the attack is targeting wholesale or retail payment systems (as detailed in section 2.3).

Members can contact the RITS Help Desk on a 24x7 basis, on 1800 659 360 or +61 2 9551 8930.

The following information should be provided during an incident:

- Advise the RITS Help Desk of communication arrangements:
    - standard contact point for the duration of the issue
    - escalation point (confirm existing contact or advise another)
- The Member should also provide information on:
    - possible cause
    - customer impact
    - systems impacted
    - recovery strategy
    - expected recovery timeframe

Ongoing communications during an incident should be by phone to the RITS Help Desk unless agreed otherwise.

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

Updates must be provided at least every 30 minutes for 'wholesale' payment incidents and every hour for retail payment incidents, unless otherwise agreed with the RITS Help Desk.

3.2 Post-Incident Reporting

A detailed post-incident report must be provided to the Reserve Bank for all reportable incidents defined above. The RITS Help Desk will confirm during or shortly after the incident whether a post-incident report is required.

The post-incident report should be provided using the Incident Report Template. Additional information, such as an incident report from a service provider, may also be attached to the report.

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 is expected to be submitted within four weeks of the incident.

The report should be emailed to the RITS Help Desk: rits@rba.gov.au. The incident report will be reviewed and a 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.

RITS MEMBER INCIDENT REPORT

Please email completed reports to the RITS Help Desk: rits@rba.gov.au.

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

Report Details:

Organisation:

RITS Member Code:

Incident Report ID:[1]

Report Status (interim or final):

Incident Contact:

Name:

Phone:

Email:

Report Authoriser:

Name:

Position:

Phone:

Email:

Date Authorised:

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

[1] In the format AAAA_DD.MM.YYYY_NN, where: AAAA is the RITS member code, DD.MM.YYYY is the incident start date, and NN is a two-digit number starting from 01 to indicate whether the incident was the first or a subsequent incident to begin on that date.

INCIDENT DETAILS	RESPONSES
Date of incident	
Incident description	
Incident root cause[2]	
Incident start time	
Incident end time	
Duration of service(s) outage	
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 was the incident 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] Select the single most relevant category from: Hardware Failure; Software/Application Failure; Network/Communications; Change Management; Infrastructure; Operational; Service Provider; Cyber-Attack/DDoS/Malware; Other.

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