Effective 1 January 2018
Version E037

AUSTRALIAN PAYMENTS NETWORK LIMITED

ABN 12 055 136 519

A Company limited by Guarantee

PROCEDURES

for

HIGH VALUE CLEARING SYSTEM FRAMEWORK

(CS4)

Commenced August 1997

Australian Payments Network Limited
Level 23, Tower 3, International Towers Sydney, 300 Barangaroo Avenue, SYDNEY NSW 2000
Telephone: (02) 9216 4888 Facsimile: (02) 9221 8057

PROCEDURES

FOR

HIGH VALUE CLEARING SYSTEM FRAMEWORK

(CS4)

INDEX

AUSTRALIAN PAYMENTS NETWORK LIMITED
ABN 12 055 136 519

A Company limited by Guarantee

Last amended effective 30/09/02

PROCEDURES

for

HIGH VALUE CLEARING SYSTEM FRAMEWORK

(CS4)

PART 1 PRELIMINARY

Definitions

1.1 The following words have these meanings in these Procedures unless the contrary intention appears.

"ACK" means Acknowledgment.

"Acknowledgment" ("ACK") means a SWIFT advice, issued by SWIFT in response to the receipt of a message in the SWIFT PDS, advising that the message has been received by SWIFT and passed all necessary validation requirements.

"Advance Information Standards Release Guide" means the document referred to as such in Clause 5.24 or such other replacement document as may be published by SWIFT from time to time.

"AEDT" means Australian Eastern Daylight Time. Inserted effective 1/01/18

"AEST" means Australian Eastern Standard Time. Inserted effective 1/01/18

"AIF" means Automated Information Facility.

"Applicant" means a person who has lodged an application for membership of the HVCS as a Framework Participant or who proposes to lodge such an application.

"AusPayNet" means Australian Payments Network Limited. Inserted effective 1/01/18

"AusPayNet PDS" means:

(a) the SWIFT PDS, and

(b) any other payment delivery system implemented by the Company from time to time,

for sending and receiving domestic high value payments in the HVCS between Framework Participants.

"Automated Information Facility" (**"AIF"**) means the service provided within RITS for the initiation and monitoring of SWIFT message based Commands, Enquiries and Unsolicited Advices. Last amended effective 1/01/18

"Back-up Computer Site" means, in relation to each Framework Participant using the SWIFT PDS, all system configuration components necessary to ensure connection to the SWIFT PDS as an alternate to the Primary Computer Site, particularly when the Primary Computer Site is not available. For the avoidance of doubt, the system components which together comprise a "Back-up Computer Site" need not be situated at the same physical location provided that, taken as a whole, those components satisfy the operational and security requirements of clauses 7.15 to 7.23 inclusive. Last amended effective 23/04/98

"Back-up Tier" means either of the two tiers of back-up referred to in Clause 7.12, and in relation to a Framework Participant, the tier of back-up applicable to that member from time to time as determined in accordance with Clauses 7.12 to 7.14 inclusive. A Framework Participant's Back-up Tier is determinative of the back-up requirements with which that member must comply. Amended effective 1/01/14

"Board" means the board of directors of the Company.

"BSB Number" means, in relation to a Framework Participant, its BSB Number assigned to it by the Company.

"Business Day" means a day on which RITS is operating to process payments. Last amended effective 1/01/18

"Bypass Mode" [Deleted] Deleted effective 20/08/04

"CAP" means Customer Access Point.

"Cash Settlement Rate" [Renamed "ESR"]. Last amended effective 13/06/01

"CBT" means computer based terminal (including hardware and software) and, in relation to an AusPayNet PDS, means a computer based terminal used to access that AusPayNet PDS.

"Central SWIFT Interface" (**"CSI"**) means the RITS interface to the SWIFT FIN Copy Service. Last amended effective 1/01/18

"Certification Test Plan" means the test plan, incorporating test scripts, produced by the Company for the purpose of obtaining System Certification in accordance with Clauses 7.36 to 7.43 inclusive, to ensure that a Framework Participant's CBT has the correct PDS configuration loaded and can successfully interact with SWIFT FIN-Copy.

"CEST" means Central European Summer Time. Inserted effective 01/07/02

"CET" means Central European Time. Inserted effective 01/07/02

"Chief Executive Officer" means the person appointed as a chief executive officer of the Company under Article 7.13 and a reference in these Procedures to the Chief Executive Officer includes a reference to a person nominated by the chief executive officer to be responsible for the matter referred to in that reference.

"Collator" [Deleted] Deleted effective 23/04/13

"Company" means Australian Payments Network Limited (A.C.N. 055 136 519).

"Core Business Hours" means the minimum period during each Business Day that a Framework Participant's CBT must be logged on to the SWIFT PDS as specified in Clause 4.4.

"Core PPS" means the specific hardware and software that is normally used by participants to generate or process the bulk of their RITS SWIFT messages, by value, for high value payments. This would include, for example, systems required for sending correspondent banking and financial markets transactions. Last amended effective 1/01/18

"CSI" means Central SWIFT Interface.

"Customer" means the customer of the Receiver into whose account payments are credited.

"Customer Access Point" (**"CAP"**) means a dedicated SWIFT access point that is located within a Framework Participant's premises and is used to access the SWIFT FIN Copy Service.

"Daily Settlement Session" has the meaning given to that term in the RITS Regulations (see Clauses 4.1 and 4.3).

"Digital Certificate 1" means the PKI digital certificate used to authenticate each SWIFT PDS payment passing between a particular Sender and the Framework Participant to which that payment is addressed. Inserted effective 31/10/07

"Digital Certificate 2" means the PKI digital certificate used to authenticate each payment passing, via the SWIFT FIN-Copy Service, between a particular Sender and the CSI or between the CSI and a particular Framework Participant to which the payment is addressed. Inserted effective 31/10/07

"Disabling Event" means: Last amended effective 1/01/18

(a) processing, communications or other failure of a technical nature;

(b) inaccessibility (total or partial) to facilities by means of which payments are sent and received; or

(c) manifestation of industrial action,

which affects, or may affect, the ability of any Framework Participant to participate to the normal and usual extent in sending and receiving payments.

"Eligible Payment" means a Payment where both the Sender and Receiver have agreed to operate in the Evening Settlement Session. Inserted effective 01/07/02

"Error of Magnitude" means an error (or a series of errors on the one exchange) of or exceeding $2 million or such other amount as may be determined from time to time by the Management Committee. Deleted effective 1/01/18 Last amended effective 16/01/09

"ESA" means Exchange Settlement Account.

"ESCA" [Deleted] Deleted effective 20/11/06

"ESCA plus NIBO Limit" [Deleted] Deleted effective 20/11/06

"ESR" means the interest rate payable by the Reserve Bank of Australia on overnight credit balances of Exchange Settlement Accounts. Last amended effective 13/06/01

Deleted effective 1/01/18

Deleted effective 1/01/18

"Evening Settlement Session" has the meaning given to that term in Clause 4.1. Inserted effective 01/07/02

"Exchange Settlement Account" (**"ESA"**) means an exchange settlement account, or similar account, maintained by a Framework Participant with the Reserve Bank of Australia.

"Exchange Settlement Cash Account" ("ESCA") [Deleted] Deleted effective 20/11/06

"Exchange Settlement Funds" has the meaning given in the RITS Regulations.

"Exchange Summary" means a summary document substantially in the form of Appendix Gin the format prescribed by the Reserve Bank of Australia. Amended effective 13/11/13

"Exchange Summary Data File Transfer Facility" [Deleted] Deleted effective 23/04/13

"Failure To Match Rules" means the rules set out in clause 9.25. Last amended effective 13/11/13

"Fallback Period" means a period declared by the Chief Executive Officer to be a Fallback Period under Clause 9.17. Last amended effective 20/08/04

"Fallback Settlement" means, in relation to a Fallback Period, the multilateral net settlement of HVCS obligations exchanged during the Fallback Period, which is facilitated by the Reserve Bank of Australia. Inserted effective 13/11/13

"Framework Participant" means a body corporate which in accordance with the Regulations is a participant in the HVCS and which is permitted, in accordance with the Regulations and these Procedures, to use the SWIFT PDS. Inserted effective 1/07/14

"Future Dated Payment" means any payment entered into the SWIFT PDS in advance of the value date for the payment.

"High Value Clearing System" ("CS4") means the framework of systems and procedures contained in the Regulations for the purpose of co-ordinating, facilitating and protecting the conduct and exchange of AusPayNet PDS payments among Framework Participants and all aspects of the related clearing cycle.

"HVCS" means High Value Clearing System (CS4).

"HSM" means Hardware Security Module: A tamper-resistant device use to guarantee safe storage of PKI secrets. The HSM can be in the form of a smartcard, USB token or a LAN based device. Inserted effective 31/10/07

"Interim Session" has the meaning given to that term in Clause 4.1. Last amended effective 1/01/18

"Inter-organisation Compensation Rules" means the document (as amended or replaced) known as the Inter-organisation Compensation Rules, Publication No. 6.1 of the Company. Inserted effective 13/06/01

"MAC" [Deleted] Deleted effective 31/10/07

"Management Committee" means the committee constituted pursuant to Part 7 of the Regulations.

"Message Authentication Code" ("MAC") [Deleted] Deleted effective 31/10/07

"Morning Settlement Session" has the meaning given to that term in the RITS Regulations (see Clauses 4.1 and 4.3).

"NAK" means Negative Acknowledgment

"Negative Acknowledgment" ("NAK") means a SWIFT advice, issued by SWIFT in response to the receipt of a message, advising that the message has been received by SWIFT and rejected on the basis that it has not met the necessary validation requirements.

"Net Interbank Obligation" ("NIBO") [Deleted] Deleted effective 20/11/06

"NIBO" [Deleted] Deleted effective 20/11/06

"9.00am Settlement" means settlement of certain multilaterally netted payment obligations by debiting and crediting Exchange Settlement Accounts at or about 9.00am or at such other time as may be prescribed by the Reserve Bank of Australia. Amended effective 23/04/13

"9.00am Settlement Session" has the meaning given to that term in Clause 4.1.

"Non Eligible Payment" means a Payment where either the Sender or Receiver or both have not agreed to operate in the Evening Settlement Session. Inserted effective 01/07/02

"PAC" [Deleted] Deleted effective 1/01/18 Deleted effective 31/10/07

"Participant Start Date" means, in relation to a Framework Participant, the date on and from which that member is entitled to use the SWIFT PDS to send and receive payments, being a date specified as such for that member by the Management Committee in accordance with the Regulations.

"Participating Member" [deleted] Deleted effective 1/07/14

"Payment" means, in relation to an AusPayNet PDS, a payment submitted via that AusPayNet PDS for settlement in RITS. Last amended effective 1/01/18

"Payments Operation Area" has, in relation to each Framework Participant using the SWIFT PDS, the meaning given in Clause 7.25.

"PPS" means the Payments Processor System which is hardware and software used to generate or process RITS SWIFT messages. Last amended effective 1/01/18

"Primary Computer Site" means, in relation to each Framework Participant using the SWIFT PDS, all system configuration components necessary to ensure connection to the SWIFT PDS on a daily basis. For the avoidance of doubt, the system components which together comprise a "Primary Computer Site" need not be situated at the same physical location provided that, taken as a whole, those components satisfy the operational and security requirements of clauses 7.2 to 7.11 inclusive. Last amended effective 23/04/98

"Proprietary Authentication Code" ("PAC") [Deleted] Deleted effective 31/10/07

"Real Time Gross Settlement" means, in respect of settlement of payment obligations in any particular settlement system, the processing and settlement of those payment obligations in that system in real time and on a gross (not net) basis.

"Receiver" means a Constitutional Corporation that receives Payments from another Framework Participant in accordance with the HVCS Regulations and Procedures once admitted into the HVCS. Last amended effective 20/11/06

"Regulations" means the regulations for the HVCS as prescribed by the Company.

"Repair Routing Code BSB" means a BSB number, assigned in accordance with Clause 8.4 (See also Clause 4.14).

"Reports Session" has the meaning given to that term in clause 4.1. Inserted effective 1/01/18

"RITS Regulations" means the regulations for RITS published from time to time by the Reserve Bank of Australia. Last amended effective 1/01/18

"RITS" means the settlement system established and operated by the Reserve Bank of Australia for Real Time Gross Settlement and includes the Central SWIFT Interface. For the avoidance of doubt, references to RITS include that system when operating to effect settlement of Payments on a Real Time Gross Settlement basis and when otherwise operating to effect settlement of payments on a deferred net settlement basis. Last amended effective 1/01/18

"RITS User Handbook" means the user guides issued by the Reserve Bank of Australia in connection with the RITS Regulations.

"Sender" means a Constitutional Corporation that sends Payments to another Framework Participant in accordance with the HVCS Regulations and Procedures once admitted into the HVCS. Last amended effective 20/11/06

"Settlement Close Session" has the meaning given to that term in the RITS Regulations (see Clauses 4.1 and 4.3).

"Settlement Day" means a day on which Payments are processed in RITS as specified in, or in accordance with, the RITS Regulations. Last amended effective 1/01/18

"Settlement Session" has the same meaning as in the RITS Regulations.

"SWIFT" means Society For Worldwide Interbank Financial Telecommunication s.c., having its registered address at Avenue Adéle, 1 B-1310 La Hulpe, Belgium.

"SWIFT Customer Security Controls Framework" means SWIFT's set of mandatory and advisory security controls for SWIFT Users as published by SWIFT from time to time. Inserted effective 1/01/18

"SWIFT Customer Security Mandatory Controls Non-Compliance Form" means the form set out at the end of the Yearly Audit Compliance Certificate (Appendix A2) Inserted effective 1/01/18
"SWIFT FIN Service" means SWIFT's core message transport and processing service described in the SWIFT User Handbook.

"SWIFT FIN-Copy Service" means the service provided by SWIFT to Framework Participants pursuant to the SWIFT Service Agreement.

"SWIFT Network" means the proprietary telecommunication network and associated software owned and utilised by SWIFT to provide communications services to its users.

"SWIFT PDS" means the SWIFT FIN-Copy Service, operating, under normal circumstances, in Y-Mode, configured with Framework Participants' CBTs to meet the processing requirements of the HVCS, together with any ancillary SWIFT services provided in connection with the SWIFT FIN-Copy Service.

"SWIFT PDS CUG" is the group of Framework Participants admitted to use the SWIFT PDS to send and receive payments.

"SWIFT PDS Log" means the record to be maintained by Framework Participants in accordance with Clause 7.33 of all system outages, changes to the SWIFT PDS configuration and system test details, which forms part of the Yearly Audit Compliance Certificate.

"SWIFT PDS Operations Manager" means the person designated as such from time to time by the Chief Executive Officer.

"SWIFT PDS System" means, in relation to a Framework Participant using the SWIFT PDS, that member's own CBT, related software and ancillary equipment used to access the SWIFT PDS and process the sending and receipt of payment instructions.

"SWIFT Service Agreement" means the agreement effective 16 December 1996 entitled Agreement between the Company and SWIFT for FIN-Copy Service Administration, pursuant to which SWIFT provides its FIN Copy Service to Framework Participants.

"SWIFT User" means a body corporate that has been granted the right to connect to the SWIFT Network in accordance with the terms and conditions set out in the by-laws of SWIFT and in the SWIFT User Handbook.

"SWIFT User Handbook" means the set of rules and procedures published from time to time by SWIFT (in whatever medium) as the "SWIFT User Handbook" governing use of SWIFT's services.

"System Administrator" means the person appointed by the Reserve Bank of Australia to supervise operation of RITS. Last amended effective 1/01/18

"System Certification" means, in relation to an AusPayNet PDS, the initial certification by the Management Committee in accordance with Part 7 of these Procedures prior to that person being permitted to send and receive payments using that AusPayNet PDS.

"System Certification Checklist" means a checklist in the form of Appendix A1 of these Procedures, to be used by Framework Participants in accordance with Part 7 of these Procedures to obtain System Certification.

"**System Compliance Certificate"** means a certificate issued pursuant to Clause 7.41 by the Management Committee to a Framework Participant which has successfully completed the process for System Certification.

"System Queue" means the RITS Queue in which each Payment (other than a Warehoused Payment) is held pending processing in RITS prior to settlement. Last amended effective 1/01/18

"Total National Transaction Value" means, in respect of an AusPayNet PDS, the aggregate value of all payments sent and received by all Framework Participants using that AusPayNet PDS. This aggregate value is determined using the statistical data collected for the purposes of and in accordance with Clause 7.13. Last amended effective 23/04/98

"Transitional Member" [Deleted] Deleted effective 20/11/06

"Transitional Period" [Deleted] Deleted effective 20/11/06

"Uninterruptable Power Supply" (**"UPS"**) means equipment or facilities which provide for the supply of a continuous source of electricity to the CBT, whether through the use of batteries, generators or any other suitable means, in the event of the loss of mains power.

"UPS" means Uninterruptable Power Supply.

"Warehoused Payments" means Future Dated Payments received by RITS and held pending the due date when the payments are placed back in the System Queue for normal processing. Last amended effective 1/01/18

"Yearly Audit Compliance Certificate" means a certificate in the form of that in Appendix A2.

"Year" means a calendar year.

Interpretation

1.2 In these Procedures:

(a) words importing any one gender include the other gender;

(b) the word person includes a firm, a body corporate, an unincorporated association or an authority;

(c) the singular includes the plural and vice versa;

(d) a reference to a statute, code or the Corporations Law (or to a provision of a statute, code or the Corporations Law) means the statute, the code, the Corporations Law or the provision as modified or amended and in operation for the time being, or any statute, code or provision enacted in lieu thereof and includes any regulation or rule for the time being in force under the statute, the code, the Corporations Law or the provision; and a reference to a specific time means that time in Sydney unless the context requires otherwise.

1.3 Words defined in the Corporations Law have, unless the contrary intention appears, the same meaning in these Procedures.

1.4 Words defined in the Regulations have, unless the contrary intention appears, the same meaning in these Procedures.

1.5 These Procedures have been determined by the Management Committee and take effect on the date specified by the Chief Executive Officer pursuant to Regulation 1.2.

1.6 Headings are inserted for convenience and do not affect the interpretation of these Procedures.

Inconsistency with Articles or Regulations

1.7 If a provision of the Regulations or these Procedures is inconsistent with a provision of the Articles, the provision of the Articles prevails.

1.8 If a provision of these Procedures is inconsistent with a provision of the Regulations, the provision of the Regulations prevails.

Governing Law

1.9 These Procedures are to be interpreted in accordance with the same laws which govern the interpretation of the Articles.

Copyright

1.10 Copyright in these Procedures is vested in the Company.

The next page is 2.1

PART 2 EFFECT

2.1 These Procedures have the effect set out in Part 2 of the Regulations.

2.2 The provisions of these Procedures apply to the Framework known or referred to as the domestic high value clearing system but only with respect to payment instructions sent and received electronically using the SWIFT PDS.

2.3 If any AusPayNet PDS other than the SWIFT PDS is to be implemented, additional separate procedures will be required for that other AusPayNet PDS.

The next page is 3.1

PART 3 PROCEDURES AND AMENDMENT

Conduct of Clearings

3.1 Pursuant to Regulation 11.1 and in addition to and subject to the Regulations, the sending and receipt of payment instructions by Framework Participants must comply with the applicable practices, procedures, standards and specifications contained in these Procedures.

Amendments

3.2 These Procedures may be varied by the Management Committee in accordance with Regulation 11.3 and Clause 3.3 of these Procedures. Any variation to these Procedures must contain an editorial note setting out the effective date of such variation.

3.3 Each Framework Participant must notify the Company of any changes to its contact points as specified in Appendices C1, C2 and C3. The Chief Executive Officer may vary Appendices C1, C2 and C3 in accordance with such notification without the need to obtain the approval of the Management Committee or any other person. A variation made by the Chief Executive Officer pursuant to this Clause 3.3 will, upon publication by the Company, be binding on that Framework Participant and each other Framework Participant.

Inconsistency With Other Applicable Rules and Regulations

3.4 Some of the provisions of these Procedures refer to or reflect the requirements of SWIFT in relation to the SWIFT PDS or the requirements of the Reserve Bank of Australia in relation to RITS. Those requirements of SWIFT or the Reserve Bank of Australia might change from time to time. Last amended effective 1/01/18

3.5 Subject to this Clause 3.5, if any provision of these Procedures is inconsistent with any mandatory provision of the SWIFT User Handbook, the provision in the SWIFT User Handbook prevails to the extent of that inconsistency. However, any provision of these Procedures which:

(a) deals with the same subject as any provision of the SWIFT User Handbook, and

(b) imposes on any Framework Participant more rigorous obligations in relation to that subject than does that provision of the SWIFT User Handbook, or removes or limits any discretion that may have been available under or in accordance with that provision of the SWIFT User Handbook in relation to that subject, or imposes additional obligations to those imposed by that provision of the SWIFT User Handbook in relation to that subject, and

(c) can be performed without breaching that other provision of the SWIFT User Handbook,

is not to be construed as inconsistent with, and accordingly prevails over, that other provision of the SWIFT User Handbook.

3.6 Any provision of these Procedures which restates terms or conditions applicable to, or which otherwise covers, operation of RITS is included for information purposes only and is not, by virtue of these Procedures only, binding under these Procedures. Framework Participants should refer to the RITS Regulations for the terms and conditions of operation of RITS. Last amended effective 1/01/18

3.7 Framework Participants should, therefore, be conversant with the relevant provisions of both the SWIFT User Handbook and RITS Regulations.

The next page is 4.1

PART 4 GENERAL OPERATIONAL REQUIREMENTS

RITS Operating Day

Last amended effective 1/01/18

4.1 The RITS operating day is made up of four distinct operating sessions plus three closed sessions to enable completion of 9.00am Settlement, preparation for the Evening Settlement Session and overnight processing. The usual times for the sessions are specified below, but the Reserve Bank may advise other times on any given day.

Last amended effective 1/01/18

Future Dated Payments (see Warehoused Payments, Clause 5.13) received by RITS at any time during the operating day will, subject to appropriate checks, be processed and stored by RITS as Warehoused Payments. Future Dated Payments entered outside of RITS operating day will be held on the SWIFT PDS queue and forwarded to RITS on the next Business Day. *NB: See Clause 5.13, Future Dated Payments may only be entered in limited circumstances.*

Last amended effective 23/04/98

Framework Participant processing arrangements for same day value payments during each of the operating sessions varies and details are set out below.

Last amended effective 3/06/99

- Morning Settlement Session 7.30am to 8.45am Monday to Friday.

Framework Participants may use the Morning Settlement Session to fund their 9.00am Settlement position and prepare for the Daily Settlement Session. SWIFT PDS payments are not available during this period. Any SWIFT PDS payments initiated during this period for same day value will be verified, to ensure they meet all appropriate checks, and held on the System Queue until commencement of the Daily Settlement Session at which time they will be considered for settlement in the normal course.

- 9.00am Settlement Session 8.45am to 9.15am Monday to Friday.

Last amended effective 1/01/18

Only RITS processing associated with the 9.00am Settlement will be undertaken during the 9.00am Settlement Session.

Last amended effective 13/07/01

- Daily Settlement Session 9.15am to 4.30pm Monday to Friday.

Last amended effective 1/01/18

Framework Participants may initiate SWIFT PDS payments for same day value up until the close of the SWIFT PDS operating day in accordance with Clause 4.2. However, RITS will continue to be available for RITS "bank to bank" transactions until the end of the Settlement Close Session.

Last amended effective 13/07/01

- Settlement Close Session 4.30pm to 5.15pm Monday to Friday.

Inserted effective 1/01/18

Framework Participants may continue to test and settle already queued SWIFT PDS payments, and may initiate new Eligible Payments, but no other new payments may be initiated.

It is expected that Framework Participants use reasonable endeavours to ensure that Non Eligible Payments remaining on the System Queue following closure of the Daily Settlement Session are settled. This will assist all Framework Participants in managing their end of day liquidity requirements.

Last amended effective 1/01/18

At the end of the Settlement Close Session, on completion of transaction testing, RITS will reject all unsettled Non Eligible Payments remaining on the System Queue using an Abort Notification (see Clause 5.17), including payments with a status of "Deferred".

Last amended effective 1/01/18

- Interim Session approximately 5.15pm to 5.25pm Monday to Friday.

No transaction processing occurs during the Interim Session. This session is designed to allow those Framework Participants, who have not agreed to participate in the Evening Settlement Session, to obtain end of day reports and finalise their day's work. Inserted effective 1/07/02

- Evening Settlement Session closure of the Interim Session (approximately 5.25pm) to 10.00pm or such later time as the Reserve Bank may prescribe from time to time Monday to Friday. Last amended effective 1/01/18

Input of SWIFT payments will cut-off *prior* to the end of the Evening Settlement Session, at 6.05pm / 7.05pm / 8.05pm *(refer clause 4.4A). Eligible Payments remaining on the System Queue at 6.30pm / 7.30pm / 8.30pm will be rejected. Last amended effective 11/11/13

Those members that have agreed with the Reserve Bank of Australia to participate in the Evening Settlement Session must have sufficient front and back office staff available for efficient inter-bank dealings during the Evening Settlement Session. Framework Participants will be able to alter this agreement with the Reserve Bank of Australia in accordance with arrangements prescribed from time to time by the Reserve Bank of Australia. Inserted effective 1/07/02

- Reports Session 10.00pm to 10.30pm or such later time as the Reserve Bank may prescribe from time to time* (refer clause 4.4A) Monday to Friday. Last amended effective 1/01/18

No transaction processing occurs during the Reports Session. This session is designed to allow Framework Participants who have been operating in the Evening Settlement Session to obtain end of day reports and finalise their day's work. Last amended effective 1/01/18

RITS will issue "Time Period" advices throughout the day to those Framework Participants which have elected to receive them, advising those Framework Participants of the move to each new operational session, with the exception of the commencement of the 9.00am Settlement Session for which no advice will be issued. Last amended effective 1/01/18

SWIFT PDS Operating Day

4.2 SWIFT PDS operating hours for the sending of payments are: Last amended effective 23/04/98

9.15am to 4.30pm Monday to Friday for the exchange of all applicable message types; and Last amended effective 1/07/02

until 6.05pm / 7.05pm / 8.05pm* (refer clause 4.4A) for the exchange of MT202 and associated messages for those Framework Participants that have agreed to participate in the Evening Settlement Session. Last amended effective 20/06/05

Framework Participants may initiate payments, for same day value, at any time during the SWIFT PDS operating hours specified in this Clause 4.2.

Following closure of the SWIFT PDS for the day, RITS will continue to accept same day value payments provided: Last amended effective 1/01/18

- SWIFT has sent an Acknowledgment for that MT103 payment prior to 4.30pm; Last amended effective 12/12/03
- SWIFT has sent an Acknowledgment for that MT202 payment prior to 4.30pm for Non Eligible Payments or prior to 6.05pm / 7.05pm / 8.05pm*(refer clause 4.4A) for Eligible Payments; and Last amended effective 20/06/05
- the payment is received at RITS Queue prior to 4.35pm for Non Eligible Payments and prior to 6.10pm /7.10pm/ 8.10pm* (refer clause 4.4A) for Eligible Payments. Last amended effective 1/01/18

Framework Participants will need to consider RITS cut off arrangements in evaluating an appropriate internal cut-off time for sending SWIFT PDS payments. Last amended effective 1/01/18

All payments on RITS Queue during the Settlement Close Session, will be tested and either settled or queued depending upon the status of the payment and funds availability. Non Eligible Payments remaining on the System Queue once the Settlement Close Session has closed will be rejected. Last amended effective 1/01/18

Eligible Payments remaining on the System Queue at 6.30pm / 7.30pm / 8.30pm* (refer clause 4.4A) will be rejected. Inserted effective 11/11/13

Future Dated Payments initiated on any particular Business Day after closure of the SWIFT PDS will be held on the SWIFT PDS queue pending despatch to RITS on the next Business Day. Last amended effective 1/01/18

Extension of Normal Operating Hours

4.3 RITS operating hours may be extended or varied by the System Administrator for SWIFT PDS payments where normal operations have been adversely affected by extraordinary circumstances. The System Administrator will notify all Framework Participants of such extensions or varied operating hours. Last amended effective 1/01/18

Core Business Hours

4.4 For assessment of Framework Participants' CBT availability requirements, in accordance with Clause 7.32, RITS Core Business Hours are 9.15am to 5.15pm, Monday to Friday for those Framework Participants that are not participating in the Evening Settlement Session, and 9.15am to 6.30pm / 7.30pm / 8.30pm*(refer clause 4.4A) for those Framework Participants that are participating in the Evening Settlement Session, for any day on which RITS is operational. Last amended effective 1/01/18

***NOTE in relation to processing times:** Inserted effective 1/07/02

4.4A Evening Settlement Session closure times and Reports Session start and closure times are determined with reference to Central European Time and Central European Summer Time and therefore will vary throughout the year. Last amended effective 1/01/18

As a guide Central European Summer Time commences at the end of March and concludes at the end of October. Australian Eastern Summer Time usually commences at the beginning of October and concludes at the end of March. However, the relevant commencement and conclusion dates do not always coincide. Last amended effective 1/01/18

The following table may assist Framework Participants in aligning processing times for summer time and normal time across the two time zones. Inserted effective 1/07/02

10.00am CET = 8.00pm AEDT Last amendedeffective 1/01/18

10.00am CEST = 6.00pm AEST Last amended effective 1/01/18

10.00am CEST = 7.00pm AEDT Last amended effective 1/01/18

10.00am CET = 7.00pm AEST Last amended effective 1/01/18

The closure times for the Evening Settlement Session may be varied by the Reserve Bank of Australia in consultation with AusPayNet. Any variation to the closure times for the Evening Settlement Session will result in variations to the start and closure times for the Reports Session. Last amended effective 1/01/18

The Reserve Bank of Australia will, where practicable, notify HVCS Framework Participants of any such variations in advance of the day(s) that those variations apply to. Inserted effective 18/11/02

CBT Start Up Requirement

4.5 Framework Participants must be logged on to SWIFT PDS prior to 9.15am on each day that the SWIFT PDS is open for business and remain logged on for the entire operating day.

4.6 If a Framework Participant:

- is unable to log its CBT on to SWIFT PDS for commencement of the Daily Settlement Session;
- experiences any technical or operational problem with its CBT during the then current Business Day; or
- experiences any technical problems with its Core PPS during the then current Business Day, Last amended effective 14/08/08

which prevents it from processing payments, the Framework Participant must advise details of the outage to the System Administrator (see Appendix C1) as soon as possible, but no later than 30 minutes after that Framework Participant first became aware of the problem.

Where it is considered the outage will be protracted the System Administrator will advise Framework Participants in accordance with Clause 9.6.

4.7 Where a Framework Participant has advised details of a system outage in accordance with Clause 4.6 and the problem has subsequently been corrected, that Framework Participant must advise the System Administrator that the problem has been rectified and that the Framework Participant can resume normal processing. After receiving advice from a Framework Participant under this Clause 4.7, the System Administrator will immediately advise Framework Participants of the changed circumstances.

4.8 Full details of all system outages, including the date/time, cause and duration of the problem must be recorded in the SWIFT PDS Log.

4.9 Framework Participants experiencing difficulties with their Core PPS, rather than their CBT, must ensure that the CBT remains logged on to SWIFT for the entire Business Day to allow for the receipt of inward payments. Last amended effective 14/08/08

Full details of Contingency Procedures requirements are set out in Part 9 of these Procedures.

CBT Close Down

4.10 Framework Participants must remain logged on to the SWIFT PDS on each Business Day on which RITS is operating until payments processing for the day has been completed. Once payment processing has been completed at the central site, those Framework Participants who have elected to receive Time Period Advices will receive a Time Period Advice from RITS, advising a change in operational state "RTGS System Queue Processing Complete". Last amended effective 1/01/18

Holiday Arrangements

4.11 The SWIFT PDS will be open for normal operations on any day on which RITS is operating. Last amended effective 1/01/18

An annual listing of days on which RITS will not be operating may be obtained from RITS using the AIF (see generally Part 6). Framework Participants wishing to utilise this service should refer to the RITS Regulations. Last amended effective 1/01/18

4.12 Framework Participants based in a location not experiencing a public holiday on a day on which RITS is closed will be unable to process payments for value that day. It will be a decision for individual Framework Participants as to whether they offer SWIFT PDS payment facilities on that day. Any payments to be sent on such a day will need to be entered as Future Dated Payments. Last amended effective 1/01/18

SWIFT PDS BIC/BSB Data

4.13 BIC/BSB particulars for Framework Participants will be recorded in the Company's "HVCS BIC/BSB Directory". The paper based version of the BIC/BSB Directory will list all SWIFT PDS BIC/BSB links both numerically, by BSB number, and alphabetically in Framework Participant order. Framework Participants' Repair Routing Code BSBs will be recorded alphabetically in Framework Participant order in a separate section of the Directory. File and Record Formats for the HVCS BIC/BSB Directory are set out in Appendix H. Last amended effective 23/04/98

A monthly BIC/BSB Update Report, listing all changes made to the BIC/BSB links since the last report, will also be available in electronic or paper form. File and Record Formats for the BIC/BSB Update Report are set out in Appendix H.

If a Framework Participant operates multiple SWIFT PDS BICs, that member must advise the Company of details of each BSB linked to each BIC. If the volume of data is significant, details may be provided on computer diskette in the format set out in Appendix H.

Each Framework Participant must advise the Company of any new BIC/BSB links or changes to its existing BIC/BSB details. New and amended BIC/BSB data will be activated for use within the SWIFT PDS from the effective date of the monthly amendment advice containing the changes in accordance with this Clause 4.13.

The Company will provide Framework Participants with a monthly copy of the Directory or the Update Report in either electronic or paper form. To allow Framework Participants sufficient time to amend their own files AusPayNet will provide the Directory/Update Report to Framework Participants 14 days in advance of the effective date for the new version.

Repair Routing Code BSB Processing

4.14 If a Framework Participant wants to send a payment and details of the intended Receiver are known but insufficient details are available to precisely identify the beneficiary's branch, that member may send the payment to that Receiver using that Receiver's Repair Routing Code BSB (see Clause 8.4). Use of the Repair Routing Code BSB informs the Receiver that the particulars of the payment are incomplete and that manual intervention is required.

The Sender may only forward the payment to the intended Receiver using that Receiver's Repair Routing Code BSB, after it has reasonably decided that it is impracticable to contact the originator of the payment to clarify beneficiary details.

Where the Receiver is unable to apply any payment sent to it in accordance with this Clause 4.14, the Receiver must return the payment to the Sender in accordance with Clause 4.26.

4.15 Any apparent abuse of the Repair Routing Code BSB facility should immediately be brought to the attention of the Framework Participant in question, so that corrective action can be implemented.

Continual abuse of the repair facility should be reported to the Management Committee which may take such action as it considers necessary to prevent that abuse continuing so as to protect the efficiency of the HVCS.

SWIFT PDS Log

4.16 Framework Participants must maintain a SWIFT PDS Log in which they will record details of all: Last amended effective 23/04/98

- system outages and the time required to re-establish live operations (Clause 4.6);
- alterations to their Primary and Backup Computer Site system configurations (Clause 7.2, 7.16 and 7.17); and
- the date, time, duration and results of Backup Computer Site testing (Clause 7.24).

Data from the SWIFT PDS Log will form the basis of Framework Participants' responses to selected segments of the Yearly Audit Compliance Certificate (see Appendix A2).

Central Site Automated Information Facility Destination Code

4.17 The RITS Central Site SWIFT destination code for Automated Information Facility messages (Commands, Enquires and Unsolicited messages) is RSBKAUSR. Framework Participants utilising the service must ensure that Automated Information Facility messages forwarded to RITS record the above mentioned destination code. Last amended effective 1/01/18

Full details regarding RITS Automated Information Facility are contained in the RITS Regulations. Last amended effective 1/01/18

Rules Governing Compensation Claims

4.18 Any claims among Framework Participants for compensation for which provision is made in this Part 4 in respect of payments in the HVCS, must be made in accordance with the Inter-organisation Compensation Rules, to the extent applicable, unless the Framework Participants which are parties to a particular compensation claim agree (on a case by case basis) to alternative compensation arrangements in respect of that particular claim. Last amended effective 13/06/01

Each Framework Participant must nominate, in writing, to the Company a compensation contact point for the purposes of the Inter-organisation Compensation Rules. Full details of any compensation claim made in accordance with the Inter-organisation Compensation Rules must be provided to the relevant Framework Participant's nominated compensation contact point as set out in Appendix C3. Framework Participants must promptly notify the Company in writing of any changes in the contact details of their compensation contact points not less than 5 business days prior to such changes taking effect, clearly identifying the effective date in their advice. Amended effective 01/01/12

[Original clauses 4.19 to 4.21 (inclusive) deleted. Following clauses renumbered accordingly]. Deleted effective 13/06/01

Disputes Relating to Compensation Claims

4.19 If the Framework Participants concerned are unable to agree upon any matter arising in connection with a claim for compensation in respect of a payment in the HVCS, the provisions of Part 13 of the Regulations will apply to resolution of that disagreement. Last amended effective 13/06/01

Request for Return of a Settled Payment Sent in Error

4.20 Where a Framework Participant decides (for whatever reason) that a previously settled Payment was sent in error, it may request return of that Payment from the Receiver using a SWIFT Request For Cancellation message (MT192 or MT292).

Payments settled across RITS are irrevocable and accordingly any decision to return a Payment in response to a request to do so under this Clause 4.20 rests with the Receiver. The Receiver is under no obligation under these Procedures to return a settled Payment. Last amended effective 1/01/18

4.21 Where the Receiver agrees in accordance with Clause 4.20 to return any payment or otherwise returns the payment in accordance with Clause 4.27, it must return the funds to the Sender using the same message type as the original payment order. In general, the contents of block 4 (message text) of the original payment order should be returned unaltered. However, due to the processing requirements of RITS and the need to identify these payments as returned payments, some fields will need to be changed. These are: Last amended effective 1/01/18

- Field 20, this field should contain a new transaction reference number which is unique to the Framework Participant returning the payment.
- Field 32A, if the payment is returned on a day other than the day on which it was received, this field must be changed to show the value date as the date of return, otherwise the payment will be rejected by RITS. Last amended effective 1/01/18
- Field 72, the original contents of this field must be deleted and replaced with the appropriate SWIFT codeword, as set out in the SWIFT User Handbook, plus reason codes and the transaction reference number of the original returned payment order.

Refer Appendix D Message Content for additional information regarding field usage for returned payments.

4.22 Where funds are returned in accordance with Clause 4.21, on any day after the value date of the original payment, the Sender may request compensation from the Receiver, for the Receiver's use of the funds.

On receipt of a claim in accordance with this Clause 4.22, the Receiver is obliged to pay compensation in accordance with Clause 4.18, subject to refusal justifiable on legally sustainable grounds.

Receiver Unable to Apply Payment

4.23 The procedures in Clauses 4.23 to 4.26 inclusive apply where the Receiver is unable to apply an inward payment due to incorrect or incomplete beneficiary information. Last amended effective 13/06/01

In such cases the payment must be returned:

(a) within four hours of receipt of the original payment message; or

(b) if the Receiver is unable to return the payment within that four hour period because of end of day closure of RITS, within four hours after the commencement of the next Business Day's Daily Settlement Session (see also Clause 4.25). Last amended effective 1/01/18

4.24 If the Receiver must return any payment to the Sender under Clause 4.23, the Receiver must use the same message type as used for the original payment order. In general, the contents of block 4 (message text) of the original payment order should be returned unaltered. However, due to the processing requirements of RITS and the need to identify these payments as returned payments, some fields will need to be changed. These are: Last amended effective 1/01/18

- Field 20, this field should contain a new transaction reference number which is unique to the Framework Participant returning the payment.

- Field 32A, if the payment is returned on a day other than the day on which it was received, this field must be changed to show the value date as the date of return, otherwise the payment will be rejected by RITS. Last amended effective 1/01/18

- Field 72, the original contents of this field must be deleted and replaced with the appropriate SWIFT codeword, as set out in the SWIFT User Handbook, plus reason codes and the transaction reference number of the original returned payment order.

Refer Appendix D Message Content for additional information regarding field usage for rejected payments.

4.25 Where the Receiver is unable under Clause 4.23 to return a payment on the day of receipt of it, the Sender is entitled to compensation in accordance with Clause 4.18 for the Receiver's use of the funds. Last amended effective 13/06/01

On receipt of a claim in accordance with this Clause 4.25, the Receiver is required to pay the relevant compensation, subject to refusal justifiable on legally sustainable grounds.

4.26 Any apparent breach of Clause 4.23, should immediately be brought to the attention of the Framework Participant concerned, so that corrective action can be taken by that member. Last amended effective 13/06/01

Continual breaches of Clause 4.23 by the same Framework Participant should be reported to the Management Committee.

(Note: The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) imposes pre-conditions which must be satisfied before financial institutions may initiate, pass on or take any other action to carry out electronic funds transfers instructions. Please refer to Part 5 of the Act for details.) Inserted effective 30/04/07

Incorrectly Applied Items

4.27 Where it is ascertained by either the Sender or the Receiver that a payment has been misapplied, including where it has been applied to an account other than that of the intended beneficiary because the Sender transmitted incorrect account number details on which the Receiver relied (see Clause 4.29), the Receiver must on becoming aware of the error endeavour to promptly reverse that payment from the account to which it has been applied and apply the funds to the intended account, if known, or if not known, return the funds to the Sender in accordance with Clause 4.21. Last amended effective 19/09/02

Note: It is up to the Receiver to determine whether and how Customers are to be notified or prior authorisation obtained in relation to the reversals of incorrectly applied items. Inserted effective 13/06/01

Any notification of, or other arrangements with Customers, regarding the reversal of a misapplied payment beyond any obligation otherwise imposed on the Receiver by statute, common law or these Procedures, is a proprietary matter for the Receiver.

4.28 If the Sender requests the Receiver to endeavour to reverse a payment in accordance with Clause 4.27 and the payment is reversed, but it is subsequently ascertained that the original payment was not misapplied and ought not have been reversed, then as between the Sender and Receiver the Sender bears responsibility and must indemnify the Receiver in respect of any damage or claim the Receiver may suffer arising because of the reversal of that payment. Last amended effective 19/09/02

Processing by Account Number Only Inserted effective 30/11/01

4.29 If funds have been applied by the Receiver in accordance with the account number details provided by the Sender but the funds have been applied to the wrong account, then as between the Sender and Receiver, the Receiver is not liable to compensate the Sender, any person on whose behalf the Sender sends a payment, the intended beneficiary or any other person for loss of such payment. In these circumstances, liability, if any, for compensating any person for temporary or permanent loss of such payment and for any other loss or damage which a person may suffer directly or indirectly in connection with the payment is the responsibility of the Sender. Receivers are entitled to rely solely on account number details in all circumstances, regardless whether any beneficiary name details are transmitted with the account number details or are otherwise known to the Receiver. Receivers are not obliged (including under any duty to the Sender which may but for this Clause 4.29 arise at law or in equity) to check whether account number details are correct. If a Receiver suffers loss or damage, or receives any claim for loss or damage , arising because the Receiver has relied solely on account number details provided by the Sender when processing a payment, the Sender must fully indemnify the Receiver in relation to such loss or damage or claim. Inserted effective 30/11/01

(Notes:

1. *For the purpose of this Clause 4.29, account number details means the BSB number and account number or, in the case of a Receiver which has a unique account numbers system, the account number only.* Last amended effective 21/11/09

2. *The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) requires that certain information must be included in electronic funds transfer instructions. Please refer to Part 5 of the Act for details.* Last amended effective 21/11/09

3. *Beneficiary Details contained in Sequence B of the MT202COV variant are for information only and do not constitute payment instructions to the receiving Framework Participant.)* Inserted effective 21/11/09

Requests for Back Valuation and Forward Valuation of Payments

[Original clause 4.32 deleted and the following clauses renumbered accordingly]. Deleted effective 13/06/01

4.30 Where a payment is received after its due date because the Sender despatched it late, the Sender may request the Receiver to back value the payment. On receipt of a request under this Clause 4.30 to back value a payment, the Receiver must back value that payment, subject to refusal justifiable on legally sustainable grounds. Last amended effective 13/06/01

4.31 Where a payment is back valued under Clause 4.30, the Receiver is entitled to compensation from the Sender. Last amended effective 13/06/01

4.32 Where a payment is received before its due date because the Sender despatched it early, the Sender may request the Receiver to forward value the payment. On receipt of a request under this Clause 4.32 to forward value a payment, the Receiver must forward value that payment, subject to refusal justifiable on legally sustainable grounds.

4.33 Where a payment is forward valued under Clause 4.32, the Sender is entitled to compensation from the Receiver. Last amended effective 13/06/01

4.34 Subject to Clause 4.18, a Framework Participant may claim compensation from another Framework Participant in any circumstance, additional to those set out in this Part 4, that is applicable to HVCS payments and is contemplated by the Inter-organisation Compensation Rules.

Last amended effective 13/06/01

The next page is 5.1

PART 5 SWIFT PDS CLOSED USER GROUP

Overview

5.1 The SWIFT PDS CUG uses the facilities of the SWIFT FIN-Copy Service, designed to meet the needs of high value clearing systems internationally. The SWIFT FIN-Copy Service allows each country to configure its closed user group to meet its own specific requirements. AusPayNet has worked with SWIFT to configure the SWIFT PDS to meet the Australian domestic high value clearing needs of its members. For the SWIFT PDS CUG AusPayNet's SWIFT PDS configuration allows some variation from normal SWIFT messaging, to cater for RITS requirements. Details of SWIFT PDS CUG requirements are set out in this Part 5 and in Appendix D.

Last amended effective 1/01/18

To use the SWIFT PDS to send and receive payments a Framework Participant must be a SWIFT User and must meet the mandatory security control objectives in the SWIFT Customer Security Controls Framework.

Last amended effective 1/01/18

SWIFT Membership

5.2 Each Applicant proposing to use the SWIFT PDS which is not a SWIFT User, should approach the SWIFT Regional Account Manager regarding SWIFT requirements to becoming a SWIFT User. The size and international nature of the SWIFT network requires that the connection of new SWIFT Users be carried out on set dates (March, June, September and December) each year. Because of this requirement and internal systems development by the Applicant, SWIFT advises that Applicants proposing to use the SWIFT PDS should allow at least 6 months to complete the SWIFT membership process.

SWIFT PDS Closed User Group Management

5.3 The SWIFT PDS CUG will be administered by the Company. The Company will be responsible for certification pursuant to Clauses 7.36 to 7.43 inclusive, the daily operation of the SWIFT PDS CUG and the maintenance and implementation of the HVCS Regulations and Procedures applicable to the SWIFT PDS CUG.

Applicants should contact the SWIFT PDS Operations Manager concerning requirements for HVCS membership and the requirements in relation to use of the SWIFT PDS. Copies of applicable SWIFT forms can be obtained from the Company by contacting the SWIFT PDS Operations Manager.

Last amended effective 20/06/05

SWIFT PDS CUG Membership Application - General

5.4 Applicants proposing to use the SWIFT PDS will be required to complete the applicable SWIFT forms for SWIFT PDS CUG membership for test and training and/or SWIFT PDS CUG membership for live operations (as the case may be).

Last amended effective 20/06/05

Completed forms should be returned to the SWIFT PDS Operations Manager as the Company may be required to countersign the completed forms before on-sending them to SWIFT if the Applicant is to be admitted to the SWIFT PDS CUG.

Last amended effective 20/06/05

SWIFT PDS CUG Membership Application for Test and Training

5.5 As part of their overall SWIFT PDS System development, Applicants should ensure that they apply for membership of the SWIFT PDS CUG for test and training purposes in sufficient time to ensure their system will be available for proprietary testing. A minimum of 21 days should be allowed for processing the application and inclusion of the Applicant's details in the SWIFT PDS CUG records.

As specified in Clause 5.4 Applicants must complete the applicable SWIFT forms for SWIFT PDS CUG membership for test and training and forward them to the Company's SWIFT PDS Operations Manager. If the Applicant is to be admitted to the SWIFT PDS CUG for test and training purposes, the Company will countersign the completed forms and forward them to SWIFT. SWIFT will then update the SWIFT PDS CUG test and training records using the Applicants' details on those forms. Last amended effective 20/06/05

After receipt of advice from SWIFT, the Company will inform the Applicant when SWIFT PDS CUG records have been updated and the date from which the Applicant can commence test and training in the SWIFT PDS CUG.

SWIFT PDS CUG Membership Application for Live Operations

5.6 As part of the System Certification process set out in Clause 7.36, each Applicant must complete the applicable SWIFT forms for SWIFT PDS CUG membership for live operations, and attach the completed form to the System Certification Checklist which is to be forwarded to the Company in accordance with Clause 7.39. Last amended effective 20/06/05

Where the Applicant's application for System Certification is successful the Company will, following Management Committee's approval in accordance with Regulation 5.5, forward the completed forms to SWIFT. SWIFT will then update the SWIFT PDS CUG live operations records using the Applicants' details on that form. Last amended effective 20/06/05

The Secretary will, in accordance with Regulation 5.7, advise the Applicant of the date on which the Applicant may commence participation in SWIFT PDS.

Amendment of Framework Participant SWIFT PDS CUG Details

5.7 Any Framework Participant wishing to amend its SWIFT PDS CUG details must complete the applicable SWIFT form and forward the form to the Company's SWIFT PDS Operations Manager. If the Company approves that amendment it will countersign the form and then forward it to SWIFT. Last amended effective 20/06/05

The Company will advise the Framework Participant concerned when that amendment has been carried out.

SWIFT PDS (CUG) Suspension/Withdrawal of a Framework Participant

5.8 Where a Framework Participant's membership of SWIFT PDS is terminated pursuant to Regulation 5.17 or is suspended pursuant to Regulation 5.10, the Company will immediately advise SWIFT of the change to the SWIFT PDS CUG membership, using the applicable SWIFT form. Last amended effective 20/06/05

SWIFT will confirm receipt of the applicable SWIFT form, with a further advice confirming removal of applicant data from the SWIFT PDS CUG. Last amended effective 20/06/05

SWIFT PDS CUG Framework Participant Re-entry

5.9 Where the Company revokes a Framework Participant's suspension in terms of Regulation 5.16, it must immediately advise SWIFT of the reinstatement of the member using the applicable SWIFT form. Last amended effective 20/06/05

SWIFT will confirm receipt of the applicable SWIFT form, with a further advice confirming successful implementation of applicant data. Last amended effective 20/06/05

Bank Identifier Code (BIC)

5.10 Framework Participants must have a current SWIFT BIC. Framework Participants can define multiple BICs for use within the SWIFT PDS.

5.11 Where a Framework Participant chooses to implement multiple BICs it must advise the Company of full details of the BSBs attached to each BIC in accordance with Clause 4.13.

Valid SWIFT PDS Payment Messages Last amended effective 12/12/03

5.12 Two kinds of payment messages have been authorised for use in the SWIFT PDS CUG: Last amended effective 19/11/01

- MT103 Single Customer Credit Transfer; and Inserted effective 19/11/01
- MT202 General Financial Institution Transfer.

Framework Participants must ensure that all SWIFT PDS CUG payment messages contain the FIN-Copy Service Identifier "PDS" in Field 103, in accordance with Clause 8.6.

The MT103+ variation of the MT103 Single Customer Credit Transfer will be an allowable message type within the SWIFT PDS CUG. The MT103+ is distinguished from the MT103 by the use of the code "STP" in the validation flag field (message tag 119) within the user header block (block 3). Inserted effective 19/11/01

The MT202COV variation of the MT202 General Financial Transfer will be an allowable message type within the SWIFT PDS CUG. The MT202COV is distinguished from the MT202 by the use of the code "COV" in the validation flag field (message tag 119) within the user header block (block 3). Beneficiary details contained in sequence B of the MT202COV are for information only and do not constitute payment instructions to the receiving Framework Participant. Last amended effective 21/11/09

Each Framework Participant is responsible for ensuring that payment messages, including usage and content of fields in those messages, conform to the specifications set out in Appendix D.

(Note: The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) requires that certain information must be included in electronic funds transfer instructions. Please Refer to Part 5 of the Act for details.) Inserted effective 30/04/07

Warehoused Payments

5.13 Framework Participants may enter any payment (as a Future Dated Payment) into the SWIFT PDS System provided the value date for that payment is the next Business Day. RITS determines the value date from the "Value Date" contained within Field 32A of the payment message. Last amended effective 1/01/18

Future Dated Payments will be held in the SWIFT PDS queue and forwarded to RITS on the next Business Day. Last amended effective 1/01/18

To assist Framework Participants assess liquidity requirements for the day participants may use RITS to view their own Warehoused Payments, both inward and outward (excluding inward SWIFT PDS Payments with a status of deferred) due for settlement that day, from 7.00am on. With commencement of the Daily Settlement Session (9.15am) the Payments will be placed on the System Queue and processed in the normal manner. Last amended effective 1/01/18

Framework Participants can recall Warehoused Payments utilising a Recall Request, full details of which are available in the RITS Regulations.

Recall Request

5.14 Where a SWIFT PDS payment is held on the RITS Queue or is a Warehoused Payment the Sender may seek return of the payment by issuing a Recall Request. Full details of the Recall Request (Message Based Command) procedure are available in the RITS Regulations. Last amended effective 1/01/18

Out of Hours Payments

5.15 Payments sent "for value today" but despatched to RITS after normal RITS operating hours, on any particular Business Day, will be acknowledged (ACKed) by the SWIFT Fin-Copy Service and held in the SWIFT FIN-Copy queue pending opening of RITS on the next Business Day. As the value date will no longer be valid the payment will be rejected by RITS and the SWIFT FIN-Copy Service will advise details of the rejection to the Sender. Last amended effective 1/01/18

Payments sent "for value today" but despatched to RITS, on any particular Business Day, before RITS operating hours will be acknowledged (ACKed) by the SWIFT FIN-Copy Service and held in the SWIFT FIN-Copy queue pending opening of RITS on that Business day. Last amended effective 1/01/18

Sender Notification (MT012)

5.16 On the successful settlement of a Payment, RITS will send settlement details to SWIFT FIN-Copy which will forward a Sender Notification (MT012) to the Sender advising full details of the settlement, including the Sender's ESA balance following settlement of the Payment. Last amended effective 1/01/18

Abort Notification (MT019)

5.17 When RITS is unable to process a payment it will send details of rejection of that payment to SWIFT FIN-Copy, which will forward an Abort Notification (MT019) to the Sender advising the reason for the rejection. Last amended effective 1/01/18

On closure of the Settlement Close Session, RITS will automatically reject each payment remaining on the System Queue and send details of that rejection to SWIFT FIN-Copy, which will forward an Abort Notification (MT019) to the Sender advising the reason for the rejection. Last amended effective 1/01/18

Receiver Payment Order (MT103/MT202 and variants) Last amended effective 1/01/18

5.18 On advice from RITS, of the successful settlement of a Payment, SWIFT FIN-Copy will identify the original payment message, add the settlement information (time of settlement and the ESA balance following settlement of the Payment) in Field 115, and forward the original Payment with the additional settlement particulars to the Receiver (using MT103, MT202 or their respective variants as appropriate). Last amended effective 21/11/09

A more detailed description of the SWIFT FIN-Copy message process is contained in Appendix D.

Undelivered Message Reports

5.19 The following standard SWIFT reports are issued in response to a Framework Participant's request for information concerning undelivered SWIFT FIN and SWIFT FIN-Copy messages.

- Solicited Undelivered Message Report (MT066) issued in response to a MT046;
- Undelivered Message Report at a Fixed Hour (MT082) issued in response to a MT044; and
- Undelivered Message Report at Cut-off Time (MT083) issued in response to a MT044.

Where the report is dealing with FIN-Copy messages, details of fields 431 (Message Status) and 103 (Service Code) will be present in the report. Full details regarding the above reports are available from the FIN System Messages module of the SWIFT User Handbook.

Delivery Notifications

5.20 Although not part of the standard SWIFT PDS service, the Sender can specify on an individual payment basis, whether they require advice of delivery ("Delivery Notification") or a non-delivery warning ("Non-Delivery Warning"). These advices relate to the delivery or non-delivery of the payment to the Receiver and will be delivered via the SWIFT FIN Service. Normal SWIFT fees will apply for the provision of Non-Delivery Warning (MT010) and Delivery Notification (MT011) messages.

Conditional Payments

5.21 Normal SWIFT procedures as set out in the SWIFT User Handbook will apply in relation to payments containing approved SWIFT codes in Field 72, such as "/HOLD/" for a payment requiring identification before completion.

SWIFT CUG Fees

5.22 The SWIFT fee for payments processed across the CUG, has three components:

- a Domestic FIN Message Charge;
- a Sender Notification Charge; and
- a FIN-Copy Supplement Charge.

The actual SWIFT charges will vary from time to time and Framework Participants will be advised, by SWIFT, of any changes to the CUG fee structure.

SWIFT CUG fees will be invoiced as part of the normal SWIFT fee cycle.

SWIFT Archival Arrangements

5.23 SWIFT archives all sent and received messages and their associated input and delivery history for the past 123 days. Framework Participants can obtain copies of the data by instituting either a Retrieval Request (Text and History - MT020) or a Retrieval Request (History - MT022). Both messages include the Message Status (Field 431), recording the status of the original message which is being retrieved.

SWIFT Approved Standards Amendments

5.24 SWIFT operates under strict change control procedures. Amendments to the SWIFT applications normally are introduced once a year, usually in November. SWIFT publishes throughout each year several versions of its "Advance Information Standards Release Guide" advising full details of the forthcoming changes to the SWIFT FIN Service standards. The first version of the Advance Information Standards Release Guide is normally issued in or around January each year. That guide also specifies the date on which the amended standards are to be introduced, although, particularly in the early stages, it is subject to change.

If the yearly changes to SWIFT standards directly affect the SWIFT PDS, the Management Committee will advise Framework Participants of these changes and details of action required by Framework Participants.

Each Framework Participant must implement changes to that member's SWIFT PDS System in accordance with the Advance Standards Release Guide. Such changes will be reviewed when the Company reviews that member's Yearly Audit Compliance Certificate (see Clause 7.44).

Requests by Framework Participants for SWIFT PDS Amendments

5.25 If a Framework Participant wishes to propose an amendment to the existing SWIFT PDS configuration, that member should submit details of the proposal to the Company using a Change Request Form (see Appendix F), and forward the completed form to the Secretary. The details may be submitted by e-mail, using an electronic version of Appendix F (saved as a rich text format attachment). Last amended effective 30/09/02

The Secretary will acknowledge receipt of the completed Change Request Form and arrange for details to be provided to the Management Committee, which must consider the proposal as soon as reasonably practicable.

The Secretary will advise details of the Management Committee's decision to the Framework Participant which submitted the relevant Change Request Form.

SWIFT Customer Support Centre

5.26 Normal SWIFT Customer Support Centre facilities will be available should Framework Participants experience difficulties with the SWIFT system, in accordance with the SWIFT User Handbook.

The next page is 6.1

PART 6 AUTOMATED INFORMATION FACILITY

AIF Availability

6.1 RITS allows Framework Participants the scope to implement a variety of Credit and Liquidity Management mechanisms and has provided a number of Command and Enquiry options to assist Framework Participants in this regard. A full range of Commands and Enquiries is available on RITS. However, for those Framework Participants which wish to automate their payments processing, a sub-set of Commands and Enquiries is available via the SWIFT FIN service utilising RITS Automated Information Facility (AIF). Last amended effective 1/01/18

The availability of separate Credit (Credit Status) and Liquidity (ESA Status) controls, allows Framework Participant's payment areas to release payments to the System Queue independently of any decision by that member's Credit and Liquidity areas. Each Framework Participant must decide whether it will utilise the AIF and, if so, where within its organisation these facilities would be best administered.

6.2 A range of RITS AIF Unsolicited Messages and Reports are also available to Framework Participants via the SWIFT FIN service. Last amended effective 1/01/18

6.3 Framework Participants requiring further information on the AIF should refer to the RITS Regulations and RITS User Handbook.

The next page is 7.1

PART 7 FRAMEWORK PARTICIPANT TECHNICAL REQUIREMENTS

Environmental Requirements

7.1 To safeguard the SWIFT PDS and Framework Participants' interests with respect to their participation in the HVCS, it is necessary to impose certain minimum operational and security requirements on each Framework Participant's SWIFT PDS System environment. Each Framework Participant using the SWIFT PDS is required to meet specified standards in the following key areas in accordance with this Part 7: Last amended effective 23/04/98

- Primary Computer Site - Clauses 7.2 to 7.11 inclusive;
- Back-up Computer Site - Clause 7.12 to 7.24 inclusive;
- Payments Operation Area - Clause 7.25 to 7.30 inclusive; and
- Availability and Throughput Requirements - Clauses 7.31 to 7.34 inclusive.

Primary Computer Site Overview

7.2 Each Framework Participant's Primary Computer Site configuration must include the hardware required to operate its primary CBT. Each Framework Participant must ensure that all areas housing components of its Primary Computer Site configuration are secure and that access to the area is controlled by a keypad, swipe card or similar security device. Last amended effective 23/04/98

Every component of the Primary Computer Site configuration must be appropriately protected against fire, flood and water damage.

The CBT hardware, and any related hardware included in each Framework Participant's Primary Computer Site configuration which is essential to the continuous operation and availability of that member's SWIFT PDS System, must have an Uninterruptable Power Supply.

All alterations to each Framework Participant's Primary Computer Site configuration since the date of its last Yearly Audit Compliance Certificate, or if it has not previously given a Yearly Audit Compliance Certificate, the date of its System Certification Checklist, are to be recorded in its SWIFT PDS Log. Last amended effective 18/04/05

Primary Hardware and Software Requirements

7.3 Each Framework Participant's Primary Computer Site hardware and software configuration must be capable of meeting the minimum throughput requirements specified in Clause 7.34.

7.4 Each Framework Participant must maintain SWIFT certified CBT software used to allow access to the SWIFT PDS. The CBT must be SWIFT FIN-Copy compliant, that is, it must be able to load the SWIFT PDS configuration.

7.5 A back-up of the CBT software must be kept off-site for recovery purposes. Last amended effective 18/04/05

7.6 [Deleted] Deleted effective 31/10/07

Primary Security Requirements

7.7 Each Primary Computer Site must have a minimum of one HSM (Hardware Security Module) to enable Secure Login, Select (SLS) functions using PKI (Public Key Infrastructure). Last amended effective 31/10/07

7.8 A second HSM is required to provide system redundancy. Last amended effective 31/10/07

The second HSM must be tested a minimum of once every six months. Last amended effective 31/10/07

7.9 Access to all HSMs, including at the Back-up Computer Site (see Clause 7.21), must be restricted to authorised personnel only. Last amended effective 31/10/07

Primary Operating System Security

7.10 Each Framework Participant must ensure that the operating system security under which its CBT runs provides as a minimum the same functionality as the Information Technology Security Evaluation Criteria (ITSEC) rating of "E2" or the Trusted Computer System Evaluation Criteria (TCSEC) rating of "C2". The functionality of E2 and C2 security is specified in Appendix E. Last amended effective 3/06/99

Primary Site Communication Requirements Deleted effective 18/04/05

SWIFTNet IP network Inserted effective 13/10/03

7.11 Each Framework Participant must have two differently routed communication lines, each to a separate SWIFT Point of Presence (POP), ie. a primary line and a secondary line. The required communication lines can use any combination of the three available options, Public Switch Telephone Network (dial-up), leased line or Integrated Services Digital Network (dial-up). Last amended effective 18/04/05

If the adopted configuration makes use of two of the same communications options, to negate the possibility of a single point of failure they must either:

1. Be sourced from a separate service provider for each facility; or

2. If the same service provider is used then connectivity must be through diverse connection points.

Secondary communication lines to the Primary Computer Site must be tested at least four times a year at intervals of no less than two months.

Back-up Computer Requirements

7.12 Each Framework Participant must have a Back-up Computer Site configuration which includes the hardware, software and ancillary equipment required to recover that member's SWIFT PDS System operations if its Primary Computer Site fails. Last amended effective 23/04/98

The level of back-up computer support that a Framework Participant must have is dependent upon the value of SWIFT PDS payments sent and received using the SWIFT PDS. Each Framework Participant will fall within one of the following two Backup Tiers, for the purposes of the back-up requirements of these Procedures, based on the transaction values that each processes and subject to Clauses 7.13 and 7.14. The two Back-up Tiers are: Amended effective 1/01/14

Tier 1 Back-up: 2.00% or more of Total National Transaction Value;

Tier 2 Back-up: up to but not including 2.00% of Total National Transaction Value. Amended effective 1/01/14

Each Framework Participant must comply with the requirements for back-up specified in these Procedures for the Back-up Tier applicable to that member, as determined in accordance with this Clause 7.12.

Any Framework Participant may implement more robust back-up arrangements than those required to comply with these Procedures if that member believes it to be necessary or desirable in its particular circumstances.

The Secretary will advise each Framework Participant of the Back-up Tier applicable to that member:

(a) with any notice by the Secretary to that member under Regulation 5.7 (notification of successful HVCS membership application); and

(b) with any notice by the Secretary to that member, under Clause 7.13, of the Management Committee's decision in response to a written request by that member under that clause; and

(c) with any notice by the Secretary to that member under Clause 7.14.

Transaction Data Back-up Tier Allocation

Amended effective 1/07/14

7.13 The Company must collate and provide to the Management Committee quarterly statistical data showing each Framework Participant's percentage of Total National Transaction Value. The statistical collections will be in respect of each period of three consecutive calendar months commencing immediately following the preceding quarterly statistical collection period. Where a new Framework Participant joins the HVCS during a quarterly statistical collection period, its percentage share of Total National Transaction Value will be calculated on a pro-rata basis by reference to the actual period of membership of that Framework Participant.

Last amended effective 20/11/06

If any Framework Participant reasonably believes that it is required in accordance with Clause 7.12 to maintain Back-up Computer Site arrangements applicable for a different Back-up Tier than is appropriate for that member because its current percentage share of Total National Transaction Value is not a reasonable estimate of its likely SWIFT PDS traffic, then that member may in writing request the Management Committee to approve Back-up Computer Site arrangements complying with the back-up requirements applicable for a different Back-up Tier. The Management Committee may in its sole discretion consent to a request by a Framework Participant under this Clause 7.13, but such consent will not affect the application of Clause 7.14 to that member. The Secretary will notify each Framework Participant which lodges a written request with the Management Committee of the Management Committee's decision with respect to that request.

An Applicant for HVCS membership must provide to the Company in connection with its HVCS membership application a reasonable estimate in writing of its likely SWIFT PDS traffic. The Secretary will be entitled to rely on that member's estimate when notifying it, pursuant to Clause 7.12, of the Back-up Tier which will apply to it for that period.

Amended effective 1/07/14

Review of Member's Back-up Arrangements

7.14 The Management Committee will review the quarterly statistical data provided to it under Clause 7.13, and determine whether each Framework Participant's share of Total National Transaction Value has increased sufficiently to warrant maintenance by that member of back-up requirements applicable for a different Back-up Tier to that member's then current Back-up Tier.

Without prejudice to the generality of the foregoing, where any increase in a Framework Participant's share of National Transaction Value is such that the member would in accordance with Clause 7.13, fall within a different Back-up Tier to that member's then current Back-up Tier and that situation continues for two consecutive quarterly statistical collection periods referred to in Clause 7.13, the Management Committee will, subject to the following provisions of this Clause 7.14, assume that the member's share of National Transaction Value has permanently increased and require the member to comply with back-up requirements applicable for that different Back-up Tier.

If the Management Committee determines in accordance with this Clause 7.14 that any Framework Participant should comply with the back-up requirements applicable for a different Back-up Tier to that member's then current Back-up Tier, the Secretary will notify that member accordingly in writing.

If any Framework Participant receives a notice from the Secretary under this Clause 7.14, that member must respond to the Management Committee in writing within 30 days of the date of that notice providing either:

(a) a written undertaking to implement the new back-up requirements within six months of the Secretary's notice; or

(b) an explanation, accompanied by any available supporting evidence, as to why the quarterly statistics on which the Management Committee's decision was based are uncharacteristic of that member's likely ongoing share of Total National Transaction Value and written confirmation that the member does not reasonably expect its likely ongoing share of Total National Transaction Value to require, in accordance with Clause 7.12, back-up arrangements applicable for a different Back-up Tier to that member's then current Back-up Tier; or

(c) a request, accompanied by any available supporting evidence, for exemption by the Management Committee from compliance with the new back-up requirements on the basis that it will be substantially disadvantaged by the proposed change.

If the Management Committee receives a response from any Framework Participant in terms of sub-paragraph (b) or (c) of this Clause 7.14, it will consider that response and without unreasonable delay determine whether that member must comply with the back-up requirements applicable for a different Back-up Tier to that member's then current Back-up Tier. The Secretary will then promptly notify the Framework Participant concerned of the Management Committee's determination.

Back-up Computer Site Overview

7.15 Each Framework Participant must maintain a Back-up Computer Site suitably configured to meet the minimum back-up requirements applicable to that member under these Procedures. Each Framework Participant's back-up arrangements will involve either a:

Last amended effective 23/04/98

- geographically remote site, where each of the components of the Back-up Computer Site are differently located to the equivalent components of the Primary Computer Site; or

- same building site, where the Primary Computer Site and Back-up Computer Site are maintained in the one building.

Tier 1 Back-up - Geographically Remote Back-up Computer Site Requirements

7.16 Each Framework Participant that falls within the tier 1 Back-up Tier must maintain, as a minimum requirement, a Back-up Computer Site which is geographically remote from its Primary Computer Site, in terms of Clause 7.15, and which otherwise meets the requirements specified in this Clause 7.16.

A tier 1 Back-up Framework Participant must be able to: Last amended effective 1/01/14

(a) begin sending and receiving payments within two (2) hours in the event of a systems failure within the Primary Computer Site; or Amended effective 1/01/14

(b) switch to its Back-up Computer Site and begin sending and receiving payments within four (4) hours in the event of a site failure at the Primary Computer Site. Inserted effective 1/01/14

The Framework Participant must ensure that its Back-up Computer Site is secure from unauthorised entry and that access to the area is controlled by a keypad, swipe card or similar security device.

The Back-up Computer Site must be appropriately protected against fire, flood and water damage.

The Back-up Computer Site, including CBT hardware and any related hardware essential to the continuous operation and availability of the system, must have an Uninterruptable Power Supply.

All alterations to the Framework Participant's Back-up Computer Site configuration since the date of its last Yearly Audit Compliance Certificate, or if it has not previously given a Yearly Audit Compliance Certificate, the date of its System Certification Checklist, are to be recorded in its SWIFT PDS Log. Last amended effective 18/04/05

Tier 2 Back-up - Single Building Back-up Computer Site Requirements Amended effective 1/01/14

7.17 Each Framework Participant which falls within the tier 2 Back-up Tier must maintain, as a minimum requirement, a Back-up Computer Site which meets the requirements specified in this Clause 7.17. Each Framework Participant to which this Clause 7.17 applies may maintain a Back-up Computer Site in the same building as that member's Primary Computer Site, instead of a geographically remote site as is required for the tier 1 Back-up Tier. Each Framework Participant maintaining its Back-up Computer Site in the same building as its Primary Computer Site is not required to meet the redundancy requirements set out in Clauses 7.21 and 7.23. Amended effective 1/01/14

The Framework Participant must ensure that its Back-up Computer Site is secure from unauthorised entry and that access to the area is controlled by a keypad, swipe card or similar security device.

The Back-up Computer Site must be appropriately protected against fire, and flood and water damage.

The Back-up Computer Site, including CBT hardware and any related hardware essential to the continuous operation and availability of the system, must have an Uninterruptable Power Supply.

All alterations to the Framework Participant's Back-up Computer Site configuration since the date of its last Yearly Audit Compliance Certificate, or if it has not previously given a Yearly Audit Compliance Certificate, the date of its System Certification Checklist, are to be recorded in its SWIFT PDS Log. Last amended effective 18/04/05

A tier 2 Back-up Framework Participant must be able to: Amended effective 1/01/14

(a) begin sending and receiving payments within four (4) hours in the event of a systems failure within the Primary Computer Site; or Last amended effective 1/01/14

(b) switch to its Back-up Computer Site and begin sending and receiving payments within six (6) hours in the event of a site failure at the Primary Computer Site. Last amended effective 1/01/14

Although geographical remoteness of the Back-up Computer Site from the Primary Computer Site is not a mandatory requirement for those Framework Participants subject to tier 2 back-up requirements in accordance with Clause 7.12, those Framework Participants are encouraged to consider the merits of geographically remote back-up which is strongly recommended. Amended effective 1/01/14

Back-up Hardware and Software Requirements

7.18 Each Framework Participant's Back-up Computer Site hardware and software configuration must be capable of meeting the minimum throughput requirements specified in Clause 7.34.

7.19 Framework Participants may agree to share a Back-up Computer Site with other Framework Participants or to use a Back-up Computer Site provided by a third party, provided such arrangements are implemented in a manner which enables the Framework Participants concerned to satisfy the security and other obligations under these Procedures. Each Framework Participant entering into a shared Back-up Computer Site arrangement or using a third party to provide its Back-up Computer Site, must enter into an appropriate legally binding agreement, setting out the terms of the arrangement and ensuring the requirements set out in Clauses 7.15 to 7.17 are met.

If any Framework Participant has switched from its Primary Computer Site to its Back-up Computer Site in a shared back-up environment, all files and other data brought over to the Back-up Computer Site CBT by that Framework Participant must be irreversibly deleted/removed from the Back-up Computer Site by that Framework Participant:

(a) if that Back-up Computer Site is provided by a third party; or

(b) if that Back-up Computer Site is shared with any other Framework Participant,

immediately after processing is switched back to the first mentioned Framework Participant's Primary Computer Site.

The adequacy of each Framework Participant's Back-up Computer Site arrangements and any supporting agreement required under this Clause 7.19 will be reviewed as part of the certification process under Clauses 7.36 and 7.44.

7.20 Each Framework Participant must maintain a SWIFT certified copy of CBT software on the backup configuration.

Back-up Security Requirements

7.21 Subject to Clause 7.17 (same building Back-up Computer Site) the Back-up Computer Site must contain at least one HSM. Last amended effective 31/10/07

Back-up Operating System Security

7.22 Each Framework Participant must ensure that the operating system security under which its Back-up Computer Site CBT runs provides as a minimum the same functionality as the Information Technology Security Evaluation Criteria (ITSEC) rating of "E2" or the Trusted Computer System Evaluation Criteria (TCSEC) rating of "C2". The required security functionality based on ITSEC E2 and TCSEC C2 is specified in Appendix E. Last amended effective 3/06/99

Back-up Communication Requirements Deleted effective 18/04/05

SWIFTNet IP network Inserted effective 13/10/03

7.23 Subject to Clause 7.17 (same building Back-up Computer Site) each Framework Participant must maintain at least one communication line (lease line or dial-up) to a SWIFT POP from that member's Back-up Computer Site. This must be a separate communication line than those used at the Primary Computer Site and must be routed through a different exchange. It may connect to the same SWIFT POP(s) used by the Primary Computer Site. Last amended effective 18/04/05

Testing of Back-up Configuration

7.24 Each Framework Participant must test its Back-up Computer Site system configuration at least twice a year at intervals of no less than four months. It is recommended that the tests involve live traffic, but if Framework Participants are unable to achieve this then the test may be carried out using "test mode" traffic. Last amended effective 7/05/10

Full details of all Back-up Computer Site system tests required to be carried out under this Clause 7.24, including the dates that those tests were carried out and the results achieved, must be recorded by each Framework Participant concerned in that member's SWIFT PDS Log.

Note: SWIFT has a fallback connectivity guideline outlining a set of measures and tools adapted for each of the SWIFTNet connectivity packs. The guideline is available on the SWIFT web site. Inserted effective 19/08/05

Payments Operation Area Overview

7.25 Each Framework Participant's Payments Operation Area is that part of the member's organisation that houses its SWIFT PDS input and release terminals. Each Framework Participant must restrict access to its Payments Operations Area in accordance with Clause 7.26.

Payment Operation Area Security Requirements

7.26 Each Framework Participant must ensure that adequate security is in place within its Payments Operation Area to restrict the unauthorised entry of payments through that member's SWIFT PDS System. This must be achieved by implementing at least one of the following options:

- access to the area is controlled by a keypad, swipe card or similar security device;
- access to the CBTs contained in the area are controlled by a swipe card or similar device; or

- access to the application running on the CBTs contained in the area is controlled by the use of individual user IDs and passwords.

For payments that are manually keyed into a CBT each Framework Participant's SWIFT PDS System configuration should include two part release functionality; that is, payments should be input and released by different operators, controlled by appropriate password security.

7.27 [Deleted] Deleted effective 31/10/07

7.28 [Deleted] Deleted effective 31/10/07

7.29 [Deleted] Deleted effective 31/10/07

7.30 [Deleted] Deleted effective 31/10/07

Maintenance Requirements Deleted Effective 18/04/05

SWIFTNet IP network Inserted effective 13/10/03

7.31 To ensure the reliability of the overall SWIFT PDS and minimise outages suffered by individual Framework Participants, all software and hardware required to run any Framework Participant's CBT or to connect to and use the SWIFT PDS must at all times be covered by a current maintenance agreement with the vendor of that software or hardware or a third party maintenance provider. Such maintenance agreement must cover: Last amended effective 18/04/05

- CBT software;
- system software under which the CBT runs;
- hardware on which the CBT runs; and
- communication lines and related devices (Routers, MODEMs, controllers etc).

The maintenance requirements in this Clause 7.31 apply equally to the Primary Computer Site and Back-up Computer Site.

System Availability

7.32 Each Framework Participant must be logged on to the SWIFT PDS during the Core Business Hours (see Clause 4.4).

7.33 Each Framework Participant must maintain high reliability and achieve prompt resumption of payments processing following any disruption to its high value payments systems. This is to ensure efficient operation of the Australian payments system and maintain market liquidity. The following requirements apply to tier 1 Back-up and tier 2 Back-up respectively: Last amended effective 1/01/14

(a) Each tier 1 Back-up Framework Participant's system (which includes the CBT and the Core PPS) must meet a minimum of 99.7% up-time during the Core Business Hours on an annual basis. Last amended effective 1/01/14

Following any disruption of processing during Core Business Hours, a tier 1 Back-up Framework Participant must substantially resume payments processing in accordance with clause 7.16(a) or 7.16(b) as applicable. Last amended effective 1/01/14

Failure to resume payments processing within the timeframes prescribed in clause 7.16(a) or 7.16(b) as applicable will result in formal reporting by the Member at the next Management Committee meeting. Amended effective 1/01/14

No single outage of any tier 1 Back-up Framework Participant's CBT and/or Core PPS may exceed four (4) hours duration and the aggregate duration of all such outages of a CBT and/or Core PPS during the Year may not exceed six (6) hours for those Framework Participants that do not participate in the Evening Settlement Session and eight (8) hours for those Framework Participants that participate in the Evening Settlement Session. Last amended effective 1/01/14

(b) Each tier 2 Back-up Framework Participant's system (which includes the CBT and the Core PPS) must meet a minimum of 99.5% up-time during the Core Business Hours on an annual basis. Inserted effective 1/01/14

Following any disruption of processing during Core Business Hours, a tier 2 Back-up Framework Participant must substantially resume payments processing in accordance with clause 7.17(a) or 7.17(b) as applicable. Inserted effective 1/01/14

Failure to resume payments processing within the timeframes prescribed in clause 7.17(a) or 7.17(b) as applicable will result in formal reporting by the Member at the next Management Committee meeting. Inserted effective 1/01/14

No single outage of any tier 2 Back-up Framework Participant's CBT and/or Core PPS may exceed six (6) hours duration and the aggregate duration of all such outages of a CBT and/or Core PPS during the Year may not exceed ten (10) hours for those Framework Participants that do not participate in the Evening Settlement Session and thirteen (13) hours for those Framework Participants that participate in the Evening Settlement Session. Inserted effective 1/01/14

The Provisions of this Clause 7.33 apply equally to each Framework Participant's Primary Computer Site and Back-up Computer Site configurations.

Each Framework Participant must maintain a SWIFT PDS Log containing details of all its SWIFT PDS System outages, the nature of the problem causing each outage, the time taken to correct that problem and whether processing of payments was switched to that member's Back-up Computer Site must be maintained. The SWIFT PDS Log forms part of that Framework Participant's Yearly Audit Compliance Certificate (see Clause 7.44).

In addition to formal incident reporting to the Management Committee, Framework Participants must report any single outage of two (2) hours or more to the Company. Appendix A3 may be used for this purpose. The Company will notify the Management Committee of such outages , whether or not the outage also forms the basis of a Framework Participant's formal incident report. Amended effective 1/01/14

Minimum System Throughput Requirements Amended effective 1/07/14

7.34 Each Framework Participant's CBT must be capable of processing a minimum of 50% of its average daily SWIFT PDS transaction volume in any one hour, including both inward and outward traffic and associated Acknowledgments. Last amended effective 23/04/98

In respect of the System Certification, each Applicant must estimate its daily SWIFT PDS transaction volume, and specify that estimate in its System Certification Checklist.

The provisions of this Clause 7.34 apply equally in respect of both the Primary Computer Site and Back-up Computer Site.

Framework Participant Archival Requirements

7.35 Each Framework Participant must maintain archival records of all Payments and associated messages sent and received using the SWIFT PDS for each Business Day and must retain those records for a minimum of seven (7) years.

Initial Certification of Framework Participant's SWIFT PDS System

7.36 Each Applicant must arrange for certification of its SWIFT PDS System in accordance with Clauses 7.36 to 7.43 inclusive by completing and submitting a System Certification Checklist. The System Certification Checklist must be in the form appearing in Appendix A1 and is to be completed and signed by a duly authorised officer of the Applicant.

7.37 Copies of the System Certification Checklist and Certification Test Plan can be obtained from the Company by contacting the SWIFT PDS Operations Manager.

7.38 Each Applicant must demonstrate, by completing the test scripts contained within the Certification Test Plan, that its CBT is configured correctly and capable of processing SWIFT PDS messages in accordance with the HVCS Regulations and Procedures. The Company does not require Framework Participants to provide a hardcopy of the test results, except as set out in Clause 7.39, but a hardcopy should be produced and retained for internal audit purposes. AusPayNet may, as part of the verification process, request a Framework Participant to provide hardcopy test results to assist in evaluation of the Certification results. In the event that a Framework Participant is unable to produce the requested hardcopy results the Framework Participant will need to re-run the test in question. Full details of the certification test requirements are set out in the Certification Test Plan.

Last amended effective 23/04/98

7.39 The completed System Certification Checklist and the test result forms required in terms of the Certification Test Plan are to be provided to the SWIFT PDS Operations Manager. Where actual test results differ from the expected result and the Framework Participant believes that it has successfully completed the test, supporting evidence should be provided so that AusPayNet can ensure that no misunderstanding of the test requirements has occurred.

The Applicant must provide to the Company with that completed System Certification Checklist the applicable SWIFT form (duly completed) in accordance with Clause 5.6.

Last amended effective 20/06/05

The completed System Certification Checklist must be signed by a duly authorised officer of the Applicant. Any evidence of that authorisation which is reasonably requested by the Secretary or the Management Committee must be promptly produced to the Secretary following the request.

7.40 The Company will evaluate the test result forms, as set out in the Certification Test Plan, any test data provided in terms of Clause 7.39 and the related System Certification Checklist, within fourteen days of receipt of the completed System Certification Checklist, and provide a detailed report of its evaluation to the Applicant. If all requirements have been met, details of the successful System Certification will be provided to the Management Committee.

7.41 On acceptance of the System Certification Checklist by the Management Committee, the Secretary will promptly notify all Framework Participants of the successful System Certification and, if the relevant successful Applicant is already a Framework Participant, the date from which that successful Applicant will be entitled to send and receive payments using the SWIFT PDS.

The Management Committee will provide to the successful Applicant a System Compliance Certificate confirming and evidencing successful System Certification with respect to the SWIFT PDS.

7.42 If the certification process fails in part, the Company will provide the applicant with details of the deficiency as part of its report as specified in Clause 7.40, and request either a partial or complete re-run of the certification process, depending upon the nature of the problem. The applicant will be required to rectify all deficiencies and submit supporting evidence as required by the Company.

7.43 Upon receipt of the additional certification documentation the Company will carry out a review of the material in terms of Clause 7.41.

Yearly Audit Compliance

7.44 Each Framework Participant must submit to the Company annually a Yearly Audit Compliance Certificate, in the form of Appendix A2, by the end of January each year, such certificate to cover the prior calendar year and confirm that all SWIFT upgrades required since the last Yearly Audit Compliance Certificate have been implemented. Last amended effective 16/01/09

The Yearly Audit Compliance Certificate is to be signed by a duly authorised officer of the Framework Participant. Any evidence of that authorisation which is reasonably requested by the Secretary or the Management Committee must be promptly produced to the Secretary following that request.

See also Appendix A2 for further instructions on the procedural requirements in relation to Yearly Audit Compliance Certificates.

Failure to Meet Technical Requirements

7.45 If the Yearly Audit Compliance Certificate given by a Framework Participant in accordance with Clause 7.44 reveals that a Framework Participant has failed to meet any of the technical requirements specified in this Part 7, the Company will, subject to Clause 7.47, notify the Framework Participant of the deficiency, in writing, requesting rectification of the deficiency within 30 days of the date of that notice.

7.46 If any deficiency specified in any notice issued by the Company in accordance with Clause 7.45 is not rectified within the permitted 30 day period, the Company will advise details of the deficiency and action taken to date to the Management Committee for consideration as to what action will be taken, which could include (without limitation) suspension of the Framework Participant under Regulation 5.10.

7.47 If, in the opinion of the Chief Executive Officer, the deficiency notified in accordance with Clause 7.46 is such that it poses a risk to the efficiency or security of the HVCS, the deficiency will be reported directly to the Management Committee. The Management Committee may then take such remedial action which it considers necessary or desirable under the Regulations and these Procedures, including (without limitation) suspension of the Framework Participant under Regulation 5.10.

CBT Modifications and Upgrades

7.48 Any Framework Participant implementing any new CBT must successfully complete the normal initial certification process, in accordance with Clauses 7.36 to 7.40 inclusive, prior to implementing the new configuration.

7.49 Any Framework Participant implementing any upgrade or modification of its existing CBT, or any part of that system, must, prior to sending and receiving payments using the upgraded or modified system, ensure that the upgraded or modified system complies with minimum technical standards and specifications required under the Regulations and these Procedures.

7.50 If a Framework Participant upgrades or modifies, or proposes to upgrade or modify, its CBT, then the Management Committee may require that Framework Participant to provide to it particulars of that, or that proposed, upgrade or modification within 14 days of receipt of the Management Committee's request.

The Management Committee may then review the particulars of that, or that proposed, upgrade or modification provided to it under this Clause 7.50 and may issue such instructions as it considers necessary to ensure that the upgraded or modified CBT complies or will, after implementation of the proposed upgrade or modification, comply with the minimum technical standards and specifications required under the Regulations and these Procedures.

The next page is 8.1

PART 8 SWIFT PDS MESSAGE CONTENT SPECIFICATIONS

Overview

8.1 To provide for maximum automation of processing of Framework Participants inward payments, it is essential that SWIFT PDS payments input by the Sender conform to the message content specifications set out in this Part 8 and Appendix D. Close attention by Framework Participants to the completion of SWIFT PDS message details in accordance with these Procedures, will ensure the smooth and efficient operation of each Framework Participant's own SWIFT PDS System and the SWIFT PDS as a whole.

(Note: The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) requires that certain information must be included in electronic funds transfer instructions and that certain information must be obtained in respect of those instructions before financial institutions may initiate, pass on or take any other action to carry out the electronic funds transfer instructions. Please refer to Part 5 of the Act for details.)

Inserted effective 30/04/07

Message Preparation Guidelines

8.2 Message preparation guidelines, designed to assist in the straight through processing of SWIFT PDS payments, are set out in Appendix I. The guidelines are not mandatory, as they exceed normal SWIFT requirements, but are strongly recommended as a means of maximising the level of automation available within Framework Participants' own systems.

BSB Number

8.3 To use the SWIFT PDS each Framework Participant must have a BSB Number which will represent the ultimate destination for delivery of payments to that Framework Participant.

If an Applicant has not already been allocated a BSB Number by the Company because of its participation in another Framework (which BSB Number is also valid for the HVCS upon notification to AusPayNet to activate that BSB Number for the HVCS), that Applicant must request allocation of a BSB Number from the Company when applying to join the HVCS.

Repair Routing Code BSB

8.4 All Framework Participants must assign one BSB Number, to be known as the Repair Routing Code BSB, to which Framework Participants may direct payments if details of the intended recipient Framework Participant are known but there is insufficient information available to precisely identify the beneficiary's branch. Each Framework Participant must advise the Company of its Repair Routing Code BSB, which can be an existing BSB Number, by completing a "BSB and BIC Amendment Advice" available from the Company.

BIC/BSB Relationship

8.5 All authorised HVCS BSB Numbers must be linked to Framework Participant's BIC or BICs, where multiple BICs have been defined, and will be recorded in the Company's publication "HVCS BIC/BSB Directory". Each Framework Participant must ensure that the BIC and BSB Numbers included in SWIFT PDS payments sent by it conform to the approved arrangements as set out in the "HVCS BIC/BSB Directory".

FIN-Copy Service Code Identifier

8.6 SWIFT use an identification code called the FIN-Copy Service Code Identifier to uniquely identify the various FIN-Copy services operating within the SWIFT Network internationally.

The characters "PDS" will be the FIN Copy Service Code Identifier for the SWIFT PDS. Framework Participants must ensure that their SWIFT PDS Systems are configured to set Field 103 in the User Header Block 3 to "PDS" for all SWIFT PDS (MT103, MT202 and their variants). Last amended effective 21/11/09

Character Set

8.7 Normal SWIFT Character Set requirements, as set out in the SWIFT User Handbook, will apply for all SWIFT PDS payments.

Transaction Reference Number (TRN)

8.8 Framework Participants are responsible for ensuring that all SWIFT PDS payments contain a unique Transaction Reference Number ("TRN") (Field 20), and that the TRN is unique within any given fourteen (14) day period. Where a Framework Participant uses multiple Logical Terminals (LT) it must ensure the uniqueness of its TRNs across all LTs.

All TRNs are a maximum of 16 alpha-numeric characters in length.

8.9 To ensure the uniqueness of TRNs across individual high value systems (HVCS, RITS, Austraclear System), it has been agreed with the operators of these other high value systems that all RITS and Austraclear System TRNs will commence with a four character alpha identifier. The RITS TRN alpha identifier will be "RITS" while the Austraclear System identifier will be "ACLR". Last amended effective 18/04/05

SWIFT PDS messages will not require a TRN alpha identifier but Framework Participants must ensure that they exclude the use of "RITS" and "ACLR" alpha characters from the first four digits of their SWIFT PDS TRN generation routine.

8.10 Where a message is to be re-sent as the result of the original message being rejected by RITS, the Sender of the message to be re-sent must assign a new TRN to the re-sent message. Last amended effective 1/01/18

Value Date

8.11 Framework Participants may input payments for same day value or otherwise in accordance with Clause 5.13. RITS will ascertain the payment value date from the value date contained within the Amount Field (Field 32A) in the payment message. Last amended effective 1/01/18

Where a Framework Participant inputs a payment with a value date more than 5 Settlement Days in advance of the input date, RITS will reject the payment and SWIFT FIN-Copy will return an Abort Notification (MT019) to the Sender advising the reason for that rejection. Framework Participants should note that payments may only be entered as Future Dated Payments strictly in accordance with Clause 5.13. Last amended effective 1/01/18

Currency

8.12 Framework Participants may only send payments denominated in Australian dollars.

The next page is 9.1

PART 9 CONTINGENCY PROCEDURES

Application of Part 9

9.1 The provisions of this Part 9 are designed to enable orderly operation of the SWIFT PDS during Contingencies. During any period in which any provisions of this Part 9 apply, those provisions prevail, to the extent of any inconsistency, over any other provisions of these Procedures.

Responsibilities

9.2 Framework Participants have a responsibility to each other, and to the system as a whole, to co-operate in resolving any processing difficulties.

To the extent that such co-operation does not adversely affect its own processing environment, a Framework Participant receiving a request for assistance from any other Framework Participant, the Company or the System Administrator may not unreasonably withhold such assistance.

Nature of Contingency

9.3 Abnormal processing conditions which may occur, within the overall high value system, and need to be provided for include:

* Framework Participant system failure;
* central site failure (RITS or CSI); and
* central or partial communication failure (SWIFT FIN Service or SWIFT FIN-Copy Service).

Last amended effective 1/01/18

Framework Participant System Failure Overview

9.4 The appropriate response to a SWIFT PDS System failure at the Framework Participant level depends very much upon the nature of the problem, the time of day that the problem occurs and the level of redundancy that the Framework Participant concerned has available at its Primary Computer Site. While each Framework Participant has responsibilities regarding timely fallback to back-up arrangements, in accordance with Clauses 7.15 to 7.17, usually only that Framework Participant will be in the position to properly evaluate the problem and decide on the appropriate course of action for the particular circumstances applying at the time.

The Procedures set out in this Part 9 are designed to provide a framework within which each Framework Participant can consider its response to a particular SWIFT PDS System problem, but it is recognised that outside factors, for example the time of day that the problem occurs, might affect that Framework Participant's ability to comply. Where the circumstances are such that the Framework Participant experiencing system problems is unable to comply with any contingency procedures in this Part 9 or if any applicable provisions of this Part 9 would in the circumstances be inappropriate, the matter must be referred to the System Administrator for resolution.

Each Framework Participant experiencing problems with its SWIFT PDS System will continue to have inward settled Payments delivered to the SWIFT PDS queue pending re-establishment of its SWIFT PDS System operations. It is important that each Framework Participant resolve its system problems as soon as possible, either by correcting the problem with its Primary Computer Site or initiating fallback to its Back-up Computer Site.

Details of all CBT system or Core PPS problems that adversely affect the ability of any Framework Participant to send and receive payments must be recorded in that member's SWIFT PDS Log in accordance with Clause 4.8. Last amended effective 14/08/08

Redundancy and back-up arrangements for proprietary payment processors linked to CBTs (see also Clause 9.5) are not part of these procedures, but Framework Participants are expected to comply with normal industry best practice in these areas.

All Contingency Events to be Advised to System Administrator

9.5 Any Framework Participant experiencing any system problem which adversely affects its ability to send or receive SWIFT PDS payments must immediately advise the System Administrator in accordance with Clause 4.6. Each Framework Participant concerned must provide to the System Administrator brief details of the problem being experienced and give some indication as to when its SWIFT PDS System is likely to be operational again. This will assist the System Administrator in deciding whether or not to advise all Framework Participants of the outage.

Advice of HVCS Framework Participants Experiencing System Difficulties

9.6 If the System Administrator considers that a Framework Participant's system problems are likely to be protracted, the System Administrator is responsible for immediately advising details of the Framework Participant experiencing those problems to all HVCS Framework Participants by issuing a RITS broadcast message. Last amended effective 1/01/18

End-to-end test of fallback mode Inserted effective 18/01/16

9.6A Each Framework Participant must participate in an end-to-end test of fallback mode biennially on the dates specified by the Management Committee from time to time. Inserted effective 18/01/16

HVCS Processing Difficulties Contact Points

9.7 Framework Participants must, before using the SWIFT PDS to send or receive payments, nominate and advise the Company and the System Administrator of a contact point(s) to whom information or enquiries must be directed in the event of processing difficulties. A list of contact points is shown in Appendix C1.

HVCS Payments to Framework Participants Experiencing System Difficulties

9.8 Framework Participants with payments to be sent to any Framework Participant experiencing SWIFT PDS System difficulties will need to consider the liquidity implications of continuing to forward payments to that Framework Participant via the SWIFT PDS. Framework Participants should also consider the urgency or special requirements of any payments to be sent to any Framework Participant experiencing system problems, as payments may be delayed in the SWIFT queue for some considerable time.

Failure of Both the Primary and Back-up Configurations

9.9 If a Framework Participant's Primary Computer Site and Back-up Computer Site fails, the Framework Participant experiencing the problems will need to consider alternative arrangements for sending and receiving domestic high value payments.

Need to Re-establish CBT Connection in the Shortest Possible Time

9.10 Payments forwarded to a Framework Participant experiencing problems with its SWIFT PDS System will, subject to appropriate testing by RITS, be settled and queued on the Participant's SWIFT queue pending re-establishment of its connection. It is therefore imperative that the Framework Participant endeavour to re-establish its CBT connection either from the Primary Computer Site or Back-up Computer Site without delay. Last amended effective 1/01/18

Advise System Administrator When System Reactivated

9.11 Where any Framework Participant's SWIFT PDS System problems have been rectified, that Framework Participant must immediately advise: Amended effective 23/04/13

(a) the System Administrator; and

(b) if the System Administrator has issued a RITS broadcast message to all HVCS Framework Participants in respect of the problem, the Company;

of the change of status.

RITS or CSI Failure Overview Last amended effective 1/01/18

9.12 Both RITS and the CSI have two processors and each can withstand the failure of one of its two processors. However, if both processors should fail the system will revert to its back-up site. Until the move to processing using that back-up site is complete all RITS processing will cease. Framework Participants forwarding SWIFT PDS payments to RITS during this period will have those payments queued in the SWIFT PDS pending recovery of RITS. Last amended effective 1/01/18

Technically it is possible for the CSI to fail separately from RITS. In these circumstances other payment delivery feeder systems to RITS, such as RITS, might continue to use RITS to settle payments on a Real Time Gross Settlement basis, because those payment delivery systems are unaffected by failure of the CSI. Last amended effective 1/01/18

Advice of RITS Central Site Failure Last amended effective 1/01/18

9.13 The System Administrator is responsible for advising all Framework Participants, of any processing problems being experienced within RITS or the CSI, and any action initiated to correct the situation including the likely time until the system is again operational. Advice by the System Administrator in accordance with this Clause 9.13 will be given either by issuing a RITS broadcast message if possible or otherwise by the most expeditious means reasonably available using Framework Participant's contact points in Appendix C1. Last amended effective 1/01/18

Resynchronisation of RITS Data Base Last amended effective 1/01/18

9.14 The Reserve Bank of Australia has advised that if RITS fails and the RITS data base is corrupted, that data base including Framework Participants' ESA balances, will be recreated from separately maintained "redo logs". However, because there may be a period of several minutes after compilation of the last redo log and the actual system failure, there is a possibility that some data on previously settled Payments may be lost. In this case the Reserve Bank of Australia will contact each Framework Participant to verify the ESA balance and associated transactions. Where a difference exists between the balance quoted by the Reserve Bank of Australia and a Framework Participant's position, the figure quoted by the Reserve Bank of Australia will be final. Last amended effective 1/01/18

A difference in the ESA balance figure indicates that one or more previously "settled payments" have been lost and the Senders and Receivers of the payments in question will need to adjust their own figures accordingly and the Sender must re-send those payments. Framework Participants requiring further details should refer to the RITS Regulations and RITS User Handbook.

[New Clause 9.15 inserted. New Clause 9.15 was previously Clause 9.34. Following Clauses re-numbered accordingly – effective 20/08/04.]

Central Communications Failure (SWIFT FIN Service) Inserted effective 20/08/04

Partial Communications Failure (SWIFT FIN-Copy)

9.15 Standard SWIFT procedures set out in the SWIFT User Handbook will apply where the SWIFT Network or part of the SWIFT Network is experiencing difficulties.

If normal SWIFT fallback arrangements fail to resolve the problem and the difficulties become protracted, the System Administrator in conjunction with the Chief Executive Officer, will notify Framework Participants of the likely extent of the problem, using the contact details set out in Appendix C1, and action proposed. If a notice in accordance with this Clause 9.15 is issued it will be necessary for Framework Participants to consider alternative arrangements for the despatch of payments.

Failure of Both RITS and/or CSI Primary & Back-up Configurations Last amended effective 1/01/18

9.16 If both RITS main site and back-up site fail, or if the main CSI and back-up fail, the System Administrator will need to consider alternative means of processing payments. Last amended effective 1/01/18

The System Administrator has responsibility for advising full details of the failure and intended alternative processing arrangements to Framework Participants using a RITS broadcast message if possible or otherwise by the most expeditious means reasonably available using Framework Participant's contact points in Appendix C1. Last amended effective 1/01/18

9.16A In the event that the System Administrator issues a RITS broadcast message under either clause 9.6, clause 9.13 or clause 9.15, or otherwise notifies HVCS Framework Participants of a system problem, outage or other contingency event under any of those provisions, then the Chief Executive Officer may, if he considers it appropriate to do so, invoke the Member Incident Plan, which is available on the Company's Extranet, either by written notice to, or verbally notifying, the Management Committee. The Member Incident Plan provides a framework for Management Committee communication and consultation during applicable contingency events. If the Chief Executive Officer invokes the Member Incident Plan, the Management Committee will comply with its requirements. Last amended effective 1/01/18

Note: Clause 9.6 relates to processing problems experienced by a Framework Participant, clause 9.13 relates to problems within RITS or the CSI, and clause 9.15 relates to processing problems within the SWIFT Network. Last amended effective 1/01/18

FIN-Copy Operating in Bypass Mode – Deleted Deleted effective 20/08/04

Decision to Abandon Y-Copy Processing - Deleted Deleted effective 20/08/04

SWIFT PDS Payment Instructions Processed in Bypass Mode - Deleted Deleted effective 20/08/04

CLS Payments – Deleted Deleted effective 20/08/04

Future Dated Payments in Bypass Mode - Deleted Deleted effective 20/08/04

Deferred Status Payments in Bypass Mode - Deleted Deleted effective 20/08/04

Possible Duplicated Settlement Amounts - Deleted Deleted effective 20/08/04

Fallback Period Inserted effective 20/08/04

9.17 (a) If either the SWIFT PDS or RITS fails, or if both fail, then the Chief Executive Officer may, in consultation with the System Administrator, declare that a specified period is to be a Fallback Period. Any such declaration must be notified to Framework Participants by the System Administrator by the most expeditious means reasonably available using the Framework Participants' contact points in Appendix C1. Last amended effective 1/01/18

(b) Subject to Clause 9.17(c), a Fallback Period may be shortened or extended by the Chief Executive Officer, in consultation with the System Administrator. The System Administrator must notify any such variation to the Framework Participant.

(c) Any Fallback Period declared (or varied) under this Clause 9.17 must not terminate on any day before the cessation of operating hours for that day as provided for by Clause 4.2 or 4.3 (as applicable).

9.18 During a Fallback Period, Framework Participants may, by bilateral agreement, send and receive HVCS payments (except payments addressed to, or sent by, CLS Bank International) in an agreed format. Alternatively, an industry agreed template is available on the Company's extranet. Every HVCS payment sent and received pursuant to a bilateral agreement entered into under this Clause 9.18 is irrevocable at the time of receipt of that payment by the Receiver. For the avoidance of doubt, the reference to "receipt of that payment" in this Clause 9.18 means actual receipt by the Receiver of the hard copy or electronic form of the relevant payment instruction. Amended effective 18/01/16

Note 1: During a Fallback Period, Framework Participants should not send HVCS payments by means of instruments that fall within other clearing systems (eg. direct entry credits). Last amended effective 1.01.18

Note 2: By "bilateral agreement" what is meant that the institutions sending and receiving the HVCS payments should determine between themselves as to whether, and how, it will be done. The form of bilateral agreement is a matter for each member. The agreement may be constructed as an ongoing formal agreement between particular members or it could conceivably be an ad hoc agreement struck in any mutually suitable way between particular members at the time of the need for fallback.

9.19 Any HVCS payments sent during a Fallback Period must be labelled, by the Sender, individually or collectively (eg. on a cover sheet) as "HVCS payment instruction(s)".

9.20 Any HVCS payment labelled as a "HVCS payment instruction" in accordance with Clause 9.19 and sent during a Fallback period must include the same information content as a corresponding SWIFT PDS payment would normally have under these Procedures (see Part 8 and Appendix D).

Possible Duplicate Payments Inserted effective 20/08/04

9.21 Where Framework Participants need to use alternative means to process payments because of problems with the SWIFT PDS, they should be aware of the risk of duplicate payments, arising because some payments might have been trapped in the SWIFT PDS when the problem developed and will be despatched by the SWIFT PDS System when that system is reactivated.

Deferred Net Settlement

Amended effective 13/11/13

9.22 Subject to Clause 9.27, where RITS cannot be used to effect settlement of HVCS payments on a Real Time Gross Settlement basis, settlement must be conducted in accordance with Clauses 9.23 to 9.26.

Last amended effective 1/01/18

Method of Settlement

9.23 Settlement under Clause 9.22, between Framework Participants in respect of each HVCS payment (other than payments addressed to, or sent by, CLS Bank International) must be effected:

Last amended effective 23/04/13

(a) across Exchange Settlement Accounts using Fallback Settlement; and

Last amended 13/11/13

(b) for the net amount owing between each Framework Participant and all other Framework Participants.

Last amended 13/11/13

Payments processed by RITS, prior to the decision to move to alternative processing during a Fallback Period in accordance with Clause 9.17, are not affected by Clauses 9.23 to 9.26 inclusive as they have already been irrevocably settled. Normal RITS reports will be available to Framework Participants, using the AIF, as soon as RITS is operational.

Last amended effective 1/01/18

9.24 Each Framework Participant is responsible for separately identifying the amounts which are payable and receivable in respect of all payments sent and received by it, and for directly notifying the relevant settlement figures to the Reserve Bank of Australia in the manner provided for in this clause 9.24.

Last amended effective 13/11/13

Note: Payments addressed to, or sent by, CLS Bank International, should not be included in the relevant settlement figures, because such payments must not be processed on a deferred settlement basis.

Last amended effective 20/08/04

Each Framework Participant must provide to the Reserve Bank of Australia an Exchange Summary, specifying the aggregate gross values and volumes of all its inward payments received from each other Framework Participant and the aggregate gross values of all its outward payments sent to each other Framework Participant for the relevant Settlement Day and the net amount of those aggregate gross values. The completed Exchange Summary must be sent to the Reserve Bank of Australia in the manner and by the cut-off time prescribed by the Reserve Bank from time to time, ("**Cut-off Time**"), on the day the payments were sent and received.

Inserted effective 13/11/13

The Reserve Bank will send, in the manner prescribed by the Reserve Bank from time to time, provisional settlement figures showing all the settlement figures for counterparties up to the time of preparation. Each Framework Participant must immediately verify the figures and notify the Reserve Bank of Australia of any error.

Inserted effective 13/11/13

If the counterparty settlement figures do not agree, the Reserve Bank of Australia will apply the Failure to Match Rules set out in clause 9.25. It will then calculate for each Framework Participant a final settlement figure to be payable to or receivable by that Framework Participant (if applicable, derived from the application of the Failure to Match Rules) and after computing and making adjustments any interest which may be payable pursuant to clause 9.26, and notify that Framework Participant of its final net settlement figure in the manner prescribed by the Reserve Bank from time to time. The Framework Participant must settle for its final net settlement figure.

Inserted effective 13/11/13

Failure To Match Rules

Amended effective 13/11/13

9.25 The Failure to Match Rules are as follows:

(a) if the amount that one Framework Participant claims is owed to it by another Framework Participant is larger than the amount admitted by that other Framework Participant, the lesser amount will be accepted as the final settlement figure; Inserted effective 13/11/13

(b) in particular, if one Framework Participant does not admit that any amount is owing, or fails to provide settlement figures by the latest time allowed, the final settlement figure in that case will be zero; Inserted effective 13/11/13

(c) similarly, if each of two Framework Participants claims that the balance between them is in its favour, or if each of two Framework Participants claims that the balance between them is in favour of the other, the final settlement figure in that instance will be zero. Inserted effective 13/11/13

ESA Entries

Inserted effective 13/11/13

9.25A The Reserve Bank of Australia will apply entries to the Exchange Settlement Accounts of Framework Participants in accordance with the final settlement figures calculated in accordance with this Part 9. Amended effective 18/01/16

Interest Adjustment Where Settlement Delayed

9.26 Where settlement in respect of any exchange of any payment is (for whatever reason) effected on a day other than the day on which that payment was exchanged for value, an adjustment of interest will be made between the creditor and debtor Framework Participants in respect of that payment calculated at the ESR. Last amended effective 23/04/13

The Reserve Bank of Australia will record the net balance owing to or by each Framework Participant for each day on which it despatched settlement figures and calculate the interest on the net balance owing for the number of days elapsed until the day of settlement using the ESR applicable to each of those days during that period. Inserted effective 13/11/13

The Reserve Bank of Australia will notify each Framework Participant of the net amount due to or by it on account of such interest and include such interest each day in the Fallback Settlement amount of each Framework Participant. Inserted effective 13/11/13

Failure To Settle

9.27 The provisions of Part 12 of the Regulations apply if any Framework Participant is unable to meet its HVCS payment obligations due to be discharged at any particular Fallback Settlement. Last amended effective 13/11/13

Settlement Contact Points

9.28 The primary and fallback contact details and numbers to be used to contact the Reserve Bank of Australia and the settlement contact points for each Framework Participant are specified in Appendix C2. Each Framework Participant must notify the Reserve Bank of Australia in writing of any change to its settlement contact point (including any temporary change) at least five business days prior to the change, clearly identifying the effective date in their advice. Each Framework Participant is solely responsible for the consequences of any failure by it to notify the Reserve Bank of Australia of any change to its settlement contact point in accordance with this Clause 9.28. Last amended effective 13/11/13

Errors and Adjustments to Totals of Exchanges

9.29 All adjustments to totals caused by any error must be accounted for in the manner set out in this Clause 9.29: Last amended effective 20/08/04

(a) For each error which is an Error of Magnitude, the Receiver or the Sender, whichever first locates the error must notify the other immediately the details of the error are known. Once the error is agreed by both those Framework Participants, an adjustment (including interest calculated in accordance with Clause 9.30) must be effected as follows: Last amended effective 20/08/04

Errors of Magnitude

(i) if the error is agreed before 7.00am Sydney time on any day, then either:

(A) where RITS is not, at the time of that agreement, functioning to effect settlements on a Real Time Gross Settlement basis, the necessary adjustment must be made in the next Fallback Settlement, or Last amended effective 1/01/18

(B) where RITS is, at the time of that agreement, functioning to effect settlements on a Real Time Gross Settlement basis, the necessary adjustment must be made by sending a Payment for same day value on that day, or Last amended effective 1/01/18

(ii) if the error is agreed after 7.00am Sydney time on any day, the necessary adjustment must be made in a manner and at a time agreeable to both Framework Participants concerned, provided that if not effected earlier it must be effected either:

(A) where RITS is not, at the time of that agreement, functioning to effect settlements on a Real Time Gross Settlement basis, in the next Fallback Settlement after that day, or Last amended effective 1/01/18

(B) where RITS is, at the time of that agreement, functioning to effect settlements on a Real Time Gross Settlement basis, by sending a Payment for same day value no later than on the next Business Day, and Last amended effective 1/01/18

Errors which are not Errors of Magnitude

(b) For each error which is not an Error of Magnitude, an adjustment must be effected as follows:

(i) if the error is found on the day of receipt of the erroneous payment or within 3 Business Days after the day on which that erroneous payment was sent, then either:

(A) where RITS is not, at the time at which the error is found, functioning to effect settlements on a Real Time Gross Settlement basis the necessary adjustment must be made in a Fallback Settlement on any of those days, or Last amended effective 1/01/18

(B) where RITS is, at the time at which the error is found, functioning to effect settlements on a Real Time Gross Settlement basis the necessary adjustment must be made by sending a Payment for same day value on any of those days, or Last amended effective 1/01/18

(ii) if the error is not found on the day of receipt of the erroneous payment or within 3 Business Days after the day on which the erroneous payment was sent necessary adjustment must be made in a manner and at a time to be agreed between the Framework Participants concerned.

Interest Adjustments For Errors

9.30 The interest payable pursuant to Clause 9.29(a) will be calculated as follows: Last amended effective 20/08/04

(a) in respect of the first day - interest will be calculated at the ESR; and Last amended effective 13/06/01

(b) in respect of subsequent days - interest will be calculated at the ESR; however if, because of a rate of interest actually obtained by, lost to, or paid by either or both of those Framework Participants concerned upon the amount involved or upon an amount equivalent thereto, it would be equitable for some other rate to be applied, then such other rate will be applied. Last amended effective 13/06/01

Further Provisions Relating to Interest

9.31 If the Receiver and Sender concerned are unable to agree upon any question arising under Clause 9.29, the provisions of Regulations Part 13 will apply. Last amended effective 20/08/04

Losses

9.32 The provisions of Part 13 of the Regulations apply in all cases where a loss has to be met by reason of a conflict of opinion as to which Framework Participant was responsible for the loss. Last amended effective 20/08/04

[Original Clause 9.34 re-numbered as Clause 9.15 effective 20/08/04]

SWIFT PDS and RITS/RTGS System Failure – Deleted Deleted effective 20/08/04

[Original Clauses 9.35 to 9.39 (inclusive) have been re-numbered as Clauses 9.17 to 9.20 (inclusive) effective 20/08/04]

[Original Clause 9.40 has been deleted effective 20/08/04]

[Original Clause 9.41 has been re-numbered as Clause 9.21 effective 20/08/04]

9.33 Exchange Summary Data File Transfer Facility [Deleted] Deleted effective 23/04/13

The next page is 10.1

PART 10 TRANSITIONAL ARRANGEMENTS

[Deleted, effective 20/11/06]

The next page is A1.1

Last amended effective 20/11/06

SYSTEM CERTIFICATION CHECKLIST FOR MEMBERSHIP OF THE HIGH VALUE CLEARING SYSTEM ("HVCS") (Clause 7.36)

It is a requirement of the HVCS that Framework Participants satisfy certain system and environmental requirements specified in the HVCS Regulations and Procedures prior to sending or receiving payments. Copies of the System Certification Checklist are available from the Company and can be obtained from the SWIFT PDS Operations Manager.

The System Certification Checklist has been designed to assist applicants and particularly audit personnel to ensure that all requirements have been met. The System Certification Checklist is divided into a number of self-contained sections, each detailing a range of requirements cross-referenced to the relevant Clause of the HVCS Procedures. Each item in the System Certification Checklist requires a simple positive (tick) or negative (cross) response. Should a particular item require clarification or the provision of additional data, comment or information can be included at the foot of each section or a separate advice provided and attached to the System Certification Checklist.

If any clarification or additional information is required, regarding the certification process, applicants should contact the SWIFT PDS Operations Manager.

The System Certification Checklist must be completed and signed by a duly authorised officer for and on behalf of the Applicant.

The actual commencement date for a new Framework Participant is designated by the Management Committee at the time the membership application is approved. However, where the applicant has a preferred launch date, the completed System Certification Checklist and the related test results will need to be provided to the Company no less than four weeks prior to that date.

Certification Testing

It is strongly recommended that Framework Participants perform certification testing on both their primary and backup configurations but it is recognised that this may cause difficulties for some members where an existing production environment is being utilised. If this is the case a Framework Participant may complete its certification on a similar configuration such as a test system. Where this occurs it is expected that the test configuration will closely replicate the live environment, details of which will be provided to AusPayNet as part of the Certification Test Facesheet. A hardcopy of the test results are not required except in those cases where the actual test result differs from the expected result in which case the requirements of Clause 7.39 apply.

SYSTEM CERTIFICATION CHECKLIST

Last amended effective 1/01/18

TO: THE SWIFT PDS OPERATIONS MANAGER
AUSTRALIAN PAYMENTS NETWORK LIMITED
LEVEL 23, TOWER 3
INTERNATIONAL TOWERS SYDNEY, 300 BARANGAROO AVENUE
SYDNEY NSW 2000

RE: THE HIGH VALUE CLEARING SYSTEM FRAMEWORK (CS4)

FROM NAME OF APPLICANT ("Applicant") _____

PLACE OF INCORPORATION _____

AUSTRALIAN COMPANY NUMBER
AUSTRALIAN REGISTERED BODY NUMBER _____

REGISTERED OFFICE ADDRESS _____

NAME OF CONTACT PERSON _____

TELEPHONE NUMBER _____

FAX NUMBER _____

EMAIL ADDRESS _____

Environment - Primary Computer Site

- A HSM (Hardware Security Module) is available for PKI (Public Key Infrastructure) and Select (SLS) functions (Clause 7.7). ☐
- A SWIFT certified copy of CBT software is maintained (Clause 7.4). ☐
- A backup HSM is available (Clause 7.8). ☐
- Two SWIFT communication lines, a primary and a secondary line for redundancy purposes, are available (Clause 7.11). ☐
- Both SWIFT communication lines are encrypted (Clause 7.11). ☐
- Uninterruptable Power Supply (UPS) is available and supplied to the CBT hardware configuration (Clause 7.2). ☐
- The area is fitted with adequate protection against fire, flood and water damage (Clause 7.2). ☐
- CBT hardware is located in a physically secure area. Access to that area is controlled by a keypad, swipe card or similar device (Clause 7.2). ☐

Environment - Backup Computer Site

- **Tier 1 Back-up Applicants Only -** Backup computer site is geographically separate from the primary site (Clause 7.16). ☐
- **Tier 2 Back-up Applicants Only -** Backup computer site configuration meets requirements (Clause 7.17). ☐
- A SWIFT certified copy of CBT software is maintained (Clause 7.20). ☐
- A HSM is available for SLS functions (Clause 7.21). ☐
- **Tier 1 Back-up Framework Participant Only -** At least one SWIFT communication line is available, which is physically different from the two located at the primary site. The line must be encrypted (Clause 7.23). ☐
- UPS is available and supplied to the CBT hardware configuration (Clauses 7.16 and 7.17). ☐
- The area is fitted with adequate protection against fire, flood and water damage (Clauses 7.16 and 7.17). ☐
- CBT hardware is located in a physically secure area. Access to that area is controlled by a keypad, swipe card or similar device (Clauses 7.16 and 7.17). ☐
- The Backup configuration is capable of moving to live operations within the approved timeframe (Clauses 7.16 and 7.17). ☐
- If shared backup facilities are in place, full details of the arrangement are contained in a legally binding agreement (Clause 7.19). ☐

Environment - Payments Area

At least one of the following options must be utilised to prevent unauthorised entry of payments (Clause 7.26):

- Access to the area is controlled by a keypad, swipe card or similar device; ☐
- Access to the workstation(s) contained in the area is controlled by a swipe card or similar device; ☐
- Access to the application running on the workstation(s) is controlled by the use of individual user IDs and passwords. ☐

CBT Application

- CBT is configured with the SWIFT PDS profile (Clause 7.4). ☐
- CBT security enforces segregation of duties for data entry, i.e. the person entering the payment cannot be the same person that authorises it (Clause 7.26). ☐

Security

Last amended effective 1/01/18

- Self-attestation to the SWIFT Customer Security Controls Framework has been completed and submitted to SWIFT for each 8-character BIC operating in the PDS as per the SWIFT Customer ☐

Security Controls Policy (Clause 5.1).

- All mandatory security control objectives as defined in the SWIFT Customer Security Controls Framework have been met.[1] (Clause 5.1) ☐
- Operating system security which runs on the CBT hardware functionally conforms to ITSEC E2 or TCSEC C2 rating (Clause 7.10 and 7.22). ☐
- Access to the HSM is by authorised personnel only (Clause 7.9). ☐

System Availability Last amended effective 1/01/14

- **Tier 1 Back-up Applicants only** - the system (which includes the CBT and the Core PPS) must be available at least 99.7% of the Core Business Hours (Clause 7.33(a)). The level of system redundancy is designed to ensure: ☐
  - (i) No single outage will exceed four (4) hours (Clause 7.33(a)). ☐
  - (ii) Yearly downtime will not exceed six (6) hours for those Framework Participants that do not participate in the Evening Settlement Session and eight (8) hours for those Framework Participants that do participate in the Evening Settlement Session (Clause 7.33(a)). ☐
- **Tier 2 Back-up Applicants only** - the system (which includes the CBT and the Core PPS) must be available at least 99.5% of the Core Business Hours (Clause 7.33(b)). The level of system redundancy is designed to ensure: ☐
  - (i) No single outage will exceed six (6) hours (Clause 7.33(b)). ☐
  - (ii) Yearly downtime will not exceed ten (10) hours for those Framework Participants that do not participate in the Evening Settlement Session and thirteen (13) hours for those Framework Participants that do participate in the Evening Settlement Session (Clause 7.33(b)). ☐

System Performance

- Primary CBT is capable of processing 50% of daily transaction volume in 1 hour (Clause 7.34). ☐
- Backup CBT is capable of processing 50% of daily transaction volume in 1 hour (Clause 7.34). ☐
- Specify estimated daily transaction volume (Clause 7.34). ☐

CBT Support

- CBT and system software are fully supported by a current maintenance agreement with the vendor or third party (Clause 7.31). ☐
- CBT hardware is fully supported by a current maintenance agreement with the vendor or third party (Clause 7.31). ☐

Operations

[1] Note – if all mandatory controls have not been satisfied please complete the SWIFT Customer Security Mandatory Controls Non-compliance form.

- SWIFT PDS messages are stored on a suitable medium (tape, microfile, etc) for a minimum of 7 years (Clause 7.35). ☐
- A backup tape of the CBT software and data files is kept off-site (Clause 7.5). ☐
- A SWIFT PDS Log is maintained that details dates, times and durations of backup tests, outages and their cause, changes to either the primary or backup environments etc (Clauses 4.8, 7.2, 7.16, 7.17, 7.24 and 9.4). ☐

Certification Test Plan Results Last amended effective 14/08/08

The following Certification Test Plan forms have been completed and are attached:

- Certification Test Facesheet; ☐
- Specific Conditions Test Checklist; and ☐
- Community Test Checklist. ☐

Full details of test script results required in terms of Clause 7.39 are attached.

Full details of test script results required in terms of Clause 7.39 are attached.

REPRESENTATIONS AND UNDERTAKINGS

By executing this System Certification Checklist the Applicant:

(a) acknowledges that for the Applicant to qualify as a Framework Participant of HVCS to use the SWIFT PDS to send and receive payments under the HVCS Regulations and Procedures the Applicant must have obtained System Certification in accordance with the HVCS Regulations and Procedures and that this System Certification Checklist is required to obtain that System Certification;

(b) warrants and represents that the information contained in this completed System Certification Checklist (including without limitation the attached test results) is correct and accurately reflects the results of system testing using the appropriate test script supplied by the Company for the purpose of that testing;

(c) acknowledges that the Company and each other Framework Participant of the HVCS relies and will continue to rely on the accuracy of the information and the Applicant's representations, acknowledgments, warranties and undertakings contained in this Certification checklist; and

(d) agrees that if the Applicant is accepted as a Framework Participant and/or if the Applicant is permitted to use the SWIFT PDS to send and receive payments, then, in consideration of such acceptance as a Framework Participant and/or permission to use the SWIFT PDS, the Applicant will:

(i) immediately notify the Company if it becomes, or has become, aware that any information contained in this System Certification Checklist (including without limitation the attached test results) is wrong or misleading (including without limitation because of any omission to provide relevant additional information); and

(ii) provide to the Company with that notification full particulars of that wrong or misleading information.

Terms used in this Checklist in a defined sense have the same meanings as in the HVCS Procedures unless the context requires otherwise.

SIGNED FOR AND ON BEHALF
OF [NAME OF APPLICANT]:

_____

SIGNATURE OF AUTHORISED PERSON
By signing this System Certification Checklist the signatory states that the signatory is duly authorised to sign this System Certification Checklist for and on behalf of [NAME OF APPLICANT]

_____

NAME OF AUTHORISED PERSON (BLOCK LETTERS)

_____

OFFICE HELD

DATE:

The next page is A2.1

YEARLY AUDIT COMPLIANCE CERTIFICATE FOR CONTINUING MEMBERSHIP OF THE HIGH VALUE CLEARING SYSTEM ("HVCS) (Clause 7.44)

Last amended effective 07/05/10

It is a requirement of the HVCS that Framework Participants using the SWIFT PDS continue to meet at all times the SWIFT PDS and related environmental requirements, specified in the HVCS Regulations and Procedures. To assist with ensuring system-wide compliance, Framework Participants are required to carry out a yearly compliance audit in accordance with Clause 7.44 of the HVCS Procedures. Copies of the Yearly Audit Compliance Certificate to be given by each Framework Participant are available from the Company and can be obtained from the SWIFT PDS Operations Manager.

The Yearly Audit Compliance Certificate contains a standard checklist designed to assist Framework Participants and particularly audit personnel to ensure that all requirements have been met. The checklist is divided into a number of self-contained sections, each detailing a range of requirements cross-referenced to the relevant Clause of the HVCS Procedures. Each item in the checklist requires a simple positive (tick) or negative (cross) response. Should a particular item require clarification or the provision of additional information, comments can be included at the foot of each section or in a separate advice provided and annexed to the Yearly Audit Compliance Certificate.

Each Framework Participant is required to maintain a SWIFT PDS Log (see Clause 4.16) containing details of:

* the date, time and nature of all its system outages, and the time required to re-establish live operations;

* alterations to its Primary Computer Site or Backup Computer Site system configuration since the date of its last Yearly Audit Compliance Certificate or if it has not previously given a Yearly Audit Compliance Certificate, the date of its System Certification Checklist; and

* the date, time, duration and results of all its backup tests.

The SWIFT PDS Log will form the basis of a number of the certification checks and should be perused to ensure that complete and adequate details are recorded.

If any additional information or clarification is required the Framework Participant should contact the SWIFT PDS Operations Manager.

The Yearly Audit Compliance Certificate (including the checklist) must be completed and signed by a duly authorised officer for and on behalf of the Framework Participant.

Last amended effective 16/01/09

The Yearly Audit Compliance Certificate must be completed and returned to the Company by the end of January each year, such certificate to cover the prior calendar year and confirm that all SWIFT upgrades required since the last Yearly Audit Compliance Certificate have been implemented.

YEARLY AUDIT COMPLIANCE CERTIFICATE

Last amended effective 1/01/18

TO: THE SWIFT PDS OPERATIONS MANAGER
AUSTRALIAN PAYMENTSNETWORK LIMITED
LEVEL 23, TOWER 3
INTERNATIONAL TOWERS SYDNEY, 300 BARANGAROO AVENUESYDNEY NSW 2000

RE: THE HIGH VALUE CLEARING SYSTEM FRAMEWORK (CS4)

FROM NAME OF FRAMEWORK PARTICIPANT ("Member") _____

PLACE OF INCORPORATION _____

AUSTRALIAN COMPANY NUMBER
AUSTRALIAN REGISTERED BODY NUMBER _____

REGISTERED OFFICE ADDRESS _____

NAME OF CONTACT PERSON _____

TELEPHONE NUMBER _____

FAX NUMBER _____

EMAIL ADDRESS _____

Environment - Primary Computer Site

- A HSM (Hardware Security Module) is available for PKI (Public Key Infrastructure) and Select (SLS) functions (Clause 7.7). ☐
- A SWIFT certified copy of CBT software is maintained (Clause 7.4). ☐
- A backup HSM is available (Clause 7.8). ☐
- Two SWIFT communication lines, a primary and a secondary line for redundancy purposes, are available and both are encrypted (Clause 7.11). ☐
- Uninterruptable Power Supply (UPS) is available and supplied to the CBT hardware configuration (Clause 7.2). ☐
- The area is fitted with adequate protection against fire, flood and water damage (Clause 7.2). ☐
- CBT hardware is located in a physically secure area. Access to that area is controlled by a keypad, swipe card or similar device (Clause 7.2). ☐
- The backup HSM was tested twice during the year (Clause 7.8). ☐
- The secondary SWIFT communication line was tested on a minimum of four times during the year (Clause 7.11). ☐

Environment - Backup Computer Site

- **Tier 1 Back-up Framework Participants Only -** Backup computer site is geographically separate from the primary site (Clause 7.16). ☐
- **Tier 2 Back-up Framework Participants Only -** Backup computer site configuration meets requirements (Clause 7.17). ☐
- A SWIFT certified copy of CBT software is maintained (Clause 7.20). ☐
- A HSM is available for SLS functions (Clause 7.21). ☐
- **Tier 1 Back-up Framework Participant Only -** At least one SWIFT communication line is available, which is physically different from the two located at the primary site. The line must be encrypted (Clause 7.23). ☐
- UPS is available and supplied to the CBT hardware configuration (Clauses 7.16 and 7.17). ☐
- The area is fitted with adequate protection against fire, flood and water damage (Clauses 7.16 and 7.17). ☐
- CBT hardware is located in a physically secure area. Access to that area is controlled by a keypad, swipe card or similar device (Clauses 7.16 and 7.17). ☐
- If shared backup facilities are in place, full details of the arrangement are contained in a legally binding agreement (Clause 7.19). ☐
- **Tier 1 Back-up Framework Participant Only** - The Backup configuration's ability to move to live operations, with the required timeframes (as per clause 7.16(a)), was successfully tested at least twice during the year (Clause 7.24). ☐
- **Tier 2 Back-up Framework Participants Only** - The Backup configuration's ability to move to live operations, with the required timeframe (as per clause 7.17(a)), was successfully tested at least twice during the year (Clause 7.24). ☐

Environment - Payments Area

At least one of the following options must be utilised to prevent unauthorised entry of payments (Clause 7.26):

- Access to the area is controlled by a keypad, swipe card or similar device; ☐
- Access to the workstation(s) contained in the area is controlled by a swipe card or similar device; ☐
- Access to the application running on the workstation(s) is controlled by the use of individual user IDs and passwords. ☐

CBT Application

- CBT is configured with the SWIFT PDS profile (Clause 7.4). ☐
- CBT security enforces segregation of duties for data entry, i.e. the person entering the payment cannot be the same person that authorises it (Clause 7.26). ☐

Security

- Operating system security which runs on the CBT hardware functionally conforms to ITSEC E2 or TCSEC C2 rating (Clause 7.10 and 7.22). ☐
- Access to the HSM is by authorised personnel only (Clause 7.9). ☐

System Availability

Last amended effective 1/01/14

- **Tier 1 Back-up Framework Participants Only:**

  (i) The system (which includes the CBT and the Core PPS) was available at least 99.7% of the Core Business Hours during the last year (Clause 7.33(a)); ☐

  (ii) No single outage exceeded four (4) hours (Clause 7.33(a)); and ☐

  (iii) Yearly downtime did not exceed six (6) hours for those Framework Participants that do not participate in the Evening Settlement Session and eight (8) hours for those Framework Participants that do participate in the Evening Settlement Session (Clause 7.33(a)). ☐

- **Tier 2 Back-up Framework Participants Only:**

  (i) The system (which includes the CBT and the Core PPS) was available at least 99.5% of the Core Business Hours during the last year (Clause 7.33(b)); ☐

  (ii) No single outage exceeded six (6) hours (Clause 7.33(b)); and ☐

  (iii) Yearly downtime did not exceed ten (10) hours for those Framework Participants that do not participate in the Evening Settlement Session and thirteen (13) hours for those Framework Participants that do participate in the Evening Settlement Session (Clause 7.33(b)). ☐

System Performance

- Primary CBT is capable of processing 50% of the daily transaction volume in 1 hour (Clause 7.34). ☐
- Backup CBT is capable of processing 50% of the daily transaction volume in 1 hour (Clause 7.34). ☐

CBT Support

- CBT and system software are fully supported by a current maintenance agreement with the vendor or third party (Clause 7.31). ☐
- CBT hardware is fully supported by a current maintenance agreement with the vendor or third party (Clause 7.31). ☐

Operations

- SWIFT PDS messages are stored on a suitable medium (tape, microfile, etc) for a minimum of 7 years (Clause 7.35). ☐
- A backup of the CBT software and data files is kept off-site (Clause 7.5). ☐

SWIFT PDS Log

- A SWIFT PDS Log has been maintained and all appropriate details recorded as required in terms of these Procedures (Clause 4.16). ☐

SWIFT Approved Standards Amendments

- Yearly SWIFT standards amendments as set out in the final version of the Advance Information Standards release guide for the relevant year and which are applicable to the SWIFT PDS, have been successfully implemented as required (Clause 5.24). ☐

Amended effective 30/01/0
Inserted effective 1/01/18

SWIFT Customer Security Controls Framework

- Self-attestation to the SWIFT Customer Security Controls Framework has been completed and submitted to SWIFT for each 8-character BIC operating in the PDS as per the SWIFT Customer Security Controls Policy for the period corresponding to this annual compliance certificate (Clause 5.1). ☐

- All mandatory security control objectives as defined in the SWIFT Customer Security Controls Framework have been met.[1] (Clause 5.1). ☐

Fallback Mode Processes and Testing

Inserted effective 18/01/16

- Documented procedures exist and staff are appropriately trained in fallback mode processes that meet the requirements of Part 9 of the Procedures. ☐

Inserted effective 18/01/16

- The most recent end-to-end test of fallback mode as required under Clause 9.6A of the Procedures was undertaken. ☐

Inserted effective 18/01/16

REPRESENTATIONS AND UNDERTAKINGS

By executing this Certificate the Member:

(a) acknowledges that under the HVCS Procedures the Member is required to submit this Yearly Audit Compliance Certificate to the Company in accordance with those Procedures;

(b) warrants and represents that the information contained in this Yearly Audit Compliance Certificate is correct and accurately reflects both the information recorded in the SWIFT PDS Log maintained by the Member under the HVCS Procedures and the operational status generally of the Member's systems used for HVCS exchanges;

(c) acknowledges that the Company and each other Framework Participant of the HVCS relies and will continue to rely on the accuracy of the information and the Member's representations, acknowledgments, warranties and undertakings contained in this Yearly Audit Compliance Certificate; and

(d) undertakes to immediately notify the Company if it becomes aware that any information contained in this Yearly Audit Compliance Certificate is wrong or misleading (including without limitation because of any omission to provide relevant additional information) and to provide to the Company with that notification full particulars of that wrong or misleading information.

[1] Note – if all mandatory controls have not been satisfied please complete the SWIFT Customer Security Mandatory Controls Non-compliance form.

SIGNED FOR AND ON BEHALF OF *[NAME OF MEMBER]*:

_____

SIGNATURE OF AUTHORISED PERSON
By signing this Certificate the signatory states that the signatory is duly authorised to sign this Certificate for and on behalf of [NAME OF MEMBER]

_____

NAME OF AUTHORISED PERSON (BLOCK LETTERS)

_____

OFFICE HELD

DATE:

The next page is A2.7

SWIFT Customer Security Mandatory Controls Non-Compliance

Inserted effective 1/01/18

This form maybe used by an HVCS Framework Participant to report non-compliance of the SWIFT Customer Security Mandatory Controls. Alternatively, participants may submit to AusPayNet the information contained in their SWIFT Customer Security Control Policy self-attestation.

This form will need to be populated separately for each instance of non-compliance.

TO: RISK AND COMPLIANCE
AUSTRALIAN PAYMENTS NETWORK
LEVEL 23, TOWER 3
INTERNATIONAL TOWERS SYDNEY, 300 BARANGAROO AVE.
SYDNEY NSW 2000

or:

compliance@auspaynet.com.au

RE: THE HIGH VALUE CLEARING SYSTEM FRAMEWORK (CS4)

FROM: NAME OF FRAMEWORK PARTICIPANT ("Member") _____

NAME OF CONTACT PERSON _____

TELEPHONE NUMBER _____

EMAIL ADDRESS _____

Control Item Not Satisfied	
Explanation of Non-Compliance	
Plan to Become Compliant	
Target Compliance Date	

Please copy the table above as necessary to report multiple instances of non-compliance

The next page is A3.1

INCIDENT REPORT

Inserted effective 21/01/11

This form may be used by an HVCS Framework Participant to report a breach of Clause 7.33 as part of that Framework Participant's Yearly Audit Compliance Certificate (see Clause 7.44) or for the purposes of advising AusPayNet of any such breach prior to completion of the Yearly Audit Compliance Certificate.

TO: RISK AND COMPLIANCE
AUSTRALIAN PAYMENTS NETWORK LIMITED
LEVEL 23, TOWER 3
INTERNATIONAL TOWERS SYDNEY, 300 BARANGAROO AVENUE
SYDNEY NSW 2000

or:

compliance@auspaynet.com.au

RE: THE HIGH VALUE CLEARING SYSTEM FRAMEWORK (CS4)

FROM NAME OF FRAMEWORK PARTICIPANT ("Member") _____

NAME OF CONTACT PERSON _____

TELEPHONE NUMBER _____

FAX NUMBER _____

EMAIL ADDRESS _____

Date of the outage	
Time outage began	
Time outage ended	
Description of event	

Impact	
Type of system failure (e.g. hardware, software, network etc.)	
Steps taken to resolve and/or work around the problem (including time frames for problem determination and decisions taken and details of any contingency measures invoked, including use of Back-up system).	
Analysis of what caused the outage	
Steps taken to mitigate risk of problem occurring again (e.g. improved monitoring, quicker response times, more controls and checks, new procedures/technology, etc).	
Author of incident report & contact details	

The next page is A4.1

Guidelines for Certification when using Third Party Service Providers

Last amended effective 1.01.18

The purpose of these guidelines is to provide information to High Value Clearing System (HVCS) Framework Participants or Applicants (FP/A) who intend to use Third Party Providers (TPP) to supply the infrastructure to meet the technical requirements set out in Annexure A1 System Certification Checklist and Annexure A2 Yearly Audit Compliance Certificate.

Use of Third Party Providers for provision of a complete service (provision of primary and backup site and application software) is only available to Tier 2 Framework Participants (see clauses 7.12 and 7.19).

This document contains information on what requirements must be met by the Third Party Provider, by the Framework Participant or Applicant, or by both.

It is incumbent on the Framework Participant /Applicant to receive the appropriate signoff of these requirements from their TPP.

Environment - Primary Computer Site

	TPP	M/A
• A HSM (Hardware Security Module) is available for PKI (Public Key Infrastructure) and Select (SLS) functions (Clause 7.7).	☑	
• A SWIFT certified copy of CBT software is maintained (Clause 7.4).	☑	
• A backup HSM is available (Clause 7.8).	☑	
• Two SWIFT communication lines, a primary and a secondary line for redundancy purposes, are available and both are encrypted (Clause 7.11).	☑	☑
• Uninterruptable Power Supply (UPS) is available and supplied to the CBT hardware configuration (Clause 7.2).	☑	
• The area is fitted with adequate protection against fire, flood and water damage (Clause 7.2).	☑	
• CBT hardware is located in a physically secure area. Access to that area is controlled by a keypad, swipe card or similar device (Clause 7.2).	☑	
• The backup HSM was tested twice during the year (Clause 7.8). (A2 Requirement only)	☑	
• The secondary SWIFT communication line was tested on a minimum of four times during the year (Clause 7.11). (A2 Requirement only)	☑	☑

Environment - Backup Computer Site

• **Tier 2 Framework Participants -** Backup computer site configuration meets requirements (Clause 7.17).	☑
• A SWIFT certified copy of CBT software is maintained (Clause 7.20).	☑
• A HSM is available for SLS functions (Clause 7.21).	☑
• UPS is available and supplied to the CBT hardware configuration (Clauses 7.16 and 7.17).	☑

	TPP	M/A
• The area is fitted with adequate protection against fire, flood and water damage (Clauses 7.16 and 7.17).	☑	
• CBT hardware is located in a physically secure area. Access to that area is controlled by a keypad, swipe card or similar device (Clauses 7.16 and 7.17).	☑	
• If shared backup facilities are in place, full details of the arrangement are contained in a legally binding agreement (Clause 7.19). (A2 Requirement only)	☑	☑
• **Tier 2 Framework Participants** - The Backup configuration's ability to move to live operations, with the approved timeframe (as per clause 7.17), was successfully tested at least twice during the year (Clause 7.24). (A2 Requirement only)	☑	
Environment - Payments Area		
At least one of the following options must be utilised to prevent unauthorised entry of payments (Clause 7.26): • Access to the area is controlled by a keypad, swipe card or similar device; • Access to the workstation(s) contained in the area is controlled by a swipe card or similar device; • Access to the application running on the workstation(s) is controlled by the use of individual user IDs and passwords.		☑
CBT Application		
• CBT is configured with the SWIFT PDS profile (Clause 7.4).	☑	
• CBT security enforces segregation of duties for data entry, i.e. the person entering the payment cannot be the same person that authorises it (Clause 7.26).	☑	☑
Security		
• Operating system security which runs on the CBT hardware functionally conforms to ITSEC E2 or TCSEC C2 rating (Clause 7.10 and 7.22).		☑
• Access to the HSM is by authorised personnel only (Clause 7.9).	☑	
System Availability Last amended effective 1/01/18		
• The system (which includes the CBT and the Core PPS) was available at least 99.7% of the core RITS hours during the last year (Clause 7.33).	☑	
• No single outage exceeded 2 hours (Clause 7.33).	☑	☑
• Yearly downtime did not exceed 5 hours for those Framework Participants that do not participate in the Evening Settlement Session and 8 hours for those Framework Participants that do participate in the Evening Settlement Session (Clause 7.33).	☑	☑

System Performance

	TPP	M/A
• Primary CBT is capable of processing 50% of the daily transaction volume in 1 hour (Clause 7.34).	☑	
• Backup CBT is capable of processing 50% of the daily transaction volume in 1 hour (Clause 7.34).	☑	

CBT Support

• CBT and system software are fully supported by a current maintenance agreement with the vendor or third party (Clause 7.31).	☑	
• CBT hardware is fully supported by a current maintenance agreement with the vendor or third party (Clause 7.31).	☑	

Operations

• SWIFT PDS messages are stored on a suitable medium (tape, microfile, etc) for a minimum of 7 years (Clause 7.35).		☑
• A backup of the CBT software and data files is kept off-site (Clause 7.5).	☑	

SWIFT PDS Log

• A SWIFT PDS Log has been maintained and all appropriate details recorded as required in terms of these Procedures (Clause 4.16).	☑	☑

SWIFT Approved Standards Amendments

• Yearly SWIFT standards amendments as set out in the final version of the Advance Information Standards release guide for the relevant year and which are applicable to the SWIFT PDS, have been successfully implemented as required (Clause 5.24). (A2 Requirement only)	☑	

SWIFT Customer Security Controls Framework Inserted effective 1.01.18

• Self-attestation to the SWIFT Customer Security Controls Framework has been completed and submitted to SWIFT for each 8-character BIC operating in the PDS as per the SWIFT Customer Security Controls Policy for the period corresponding to this annual compliance certificate (Clause 5.1).		☑
• All mandatory security control objectives as defined in the SWIFT Customer Security Controls Framework have been met.[1] (Clause 5.1).	☑	☑

The next page is B1.1

[1] Note – if all mandatory controls have not been satisfied please complete the SWIFT Customer Security Mandatory Controls Non-compliance form.

Appendix B1 deleted effective 20/06/05

The next page is B2.1

Appendix B2 deleted effective 20/06/05

The next page is B3.1

Appendix B3 deleted effective 20/06/05

The next page is B4.1

Appendix B4 deleted effective 20/06/05

The next page is C1.1

APPENDIX C IS ISSUED AS A SEPARATE DOCUMENT

The next page is D.1

Appendix D is confidential

Confidential

MESSAGE CONTENT
(Clause 8.1)

Last amended effective 18/11/06

Confidential

Confidential

The next page is E.1
Appendix E is Confidential

Confidential

SWIFT PDS CBT SECURITY REQUIREMENTS
(Clauses 7.10 and 7.22)

The next page is F.1

CHANGE REQUEST FORM
(Clause 5.25)

	AusPayNet documents	***Joint documents***
Change Request Number	**AusPayNet ….**	**AusPayNet/RBA ….**
Short Title		
Priority: *(high, medium or low)*		
Project team member for Contact:		
Contact telephone number:		

(To be Completed by AusPayNet)

Document affected:	
Change requested by:	*Organisation:* *Name:* *Telephone number:*

Description of change:

Reasons for change:

Benefits/disadvantages of changing:

Benefits:

Disadvantages:

Effects of not changing:

CHANGE REQUEST FORM

TO: AUSTRALIAN PAYMENTS NETWORK LIMITED

The Secretary:

e-mail Address:

FROM: **Date sent:**

Name of Financial Institution:

Change Request Number:

AusPayNet documents: **AusPayNet**

Joint documents: **AusPayNet/RBA**

Short Title:

Priority High/Medium/Low

Project team member for Contact:

Contact phone number:

Document affected:

Change requested by: Organisation:

Name:

Telephone number:

Description of change:

Reasons for change:

Benefits/disadvantages of changing:

Benefits:

Disadvantages:

Effects of not changing:

The next page is G.1

APPENDIX G EXCHANGE SUMMARY

Appendix G is displayed on the Company's extranet

Last amended effective 18/01/16

The next page is H.1

HVCS BIC/BSB DIRECTORY
FILE AND RECORD FORMATS
(Clause 4.13)

The following functional specifications have been prepared to assist Framework Participants to make the necessary modifications to their own proprietary systems.

General Characteristics:

The electronic files will be a fixed length file produced on a 31/2" floppy disk and contain the same fields as the printed reports. There will be a header, a variable number of detail records and a trailer for each file.

Record Descriptions

Header Record

BYTE LOCATIONS	FIELD NAME	FIELD LENGTH	DATA FORMAT
1	Control Field (all zeros)	1	N (Contains "0")
2 - 9	File Effective Date	8	N (CCYYMMDD)
10 - 23	Creation Date & Time Stamp	14	N (CCYYMMDDhhmmss)
24 - 32	File update Number	9	N
33 - 209	Spare	177	AN

Detail Record

BYTE LOCATIONS	FIELD NAME	FIELD LENGTH	DATA FORMAT
1	Control Field	1	N (Contains "1")
2 - 7	BSB Number	6	N
8 - 9	BSB Usage Indicator (see Note 1 for detail)	2	AN
10 - 44	BSB Name	35	AN
45 - 79	BSB Street Address	35	AN
80 - 99	BSB City/Town/Suburb	20	AN
100 - 102	BSB State	3	AN
103 - 106	BSB Post Code	4	N
107 – 109	Framework Participant	3	AN
110 - 120	BIC	11	AN
121 - 209	Reserved for future use	89	AN

Trailer Record

BYTE LOCATIONS	FIELD NAME	FIELD LENGTH	DATA FORMAT
1	Control Field	1	N (Contains "9")
2 - 10	Number of detail records on File	9	N
11 - 209	Spare	199	AN

BIC BSB UPDATE REPORT

Record Descriptions:

Header Record

BYTE LOCATIONS	FIELD NAME	FIELD LENGTH	DATA FORMAT
1	Control Field (all zeros)	1	N (Contains "0")
2 - 9	File Effective Date	8	N (CCYYMMDD)
10 - 23	Creation Date & Time Stamp	14	N (CCYYMMDDhhmmss)
24 - 32	File update Number	9	N
33 – 209	Spare	177	AN

Detail Record

BYTE LOCATIONS	FIELD NAME	FIELD LENGTH	DATA FORMAT
1	Control Field	1	N (Contains "1")
2 - 4	Change Indicator (see Note 2 for detail)	3	AN
5 - 10	BSB Number	6	N
11 - 12	BSB Usage Indicator (see Note 1 for detail)	2	AN
13 - 47	BSB Name	35	AN
48 - 82	BSB Street Address	35	AN
83 - 102	BSB City/Town/Suburb	20	AN
103 - 105	BSB State	3	AN
106 - 109	BSB Post Code	4	N
110 - 112	Framework Participant	3	AN
113 - 123	BIC	11	AN
124 - 209	Reserved for future use	86	AN

Trailer Record

BYTE LOCATIONS	FIELD NAME	FIELD LENGTH	DATA FORMAT
1	Control Field	1	N (Contains "9")
2 - 10	Number of detail records on File	9	N
11 - 209	Spare	199	AN

Legend:

N Numeric only, left zero fill
AN Alpha/Numeric

Notes on Detail Record:

Note 1:

The BSB Usage indicator has the following values:

00 - BSB
01 - BSB Repair Routing Code

Note 2

The Change Indicator will have the following values:

ADD - if the record has been added
CHG - if the record has been changed
DEL - if the record has been deleted

The next page is I.1

Appendix I is Confidential

Confidential

-- END --