As amended to:
Effective 23 September 2024
Version 4

AUSTRALIAN PAYMENTS NETWORK LIMITED

ABN 12 055 136 519

A Company limited by Guarantee

PROCEDURES

for

HIGH VALUE CLEARING SYSTEM FRAMEWORK: VOLUME 2

(CS4)

Commenced August 1997

Australian Payments Network Limited
Telephone: (02) 9216 4888

PROCEDURES
for
HIGH VALUE CLEARING SYSTEM
ISO 20022 CLOSED USER GROUP

(CS4)

INDEX

PART 1 PRELIMINARY

1.1 Definitions

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

"9.00am Settlement" means settlement of certain multilaterally netted payment obligations by debiting and crediting ESAs at or about 9.00am or at such other time as may be prescribed by the RBA.

"**9.00am Settlement Session**" means the session running from 8:45am to 9:15am as set out in the RITS Regulations.

"**ACK**" means acknowledgment, which 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.

"**AEDT**" means Australian Eastern Daylight Time.

"**AEST**" means Australian Eastern Standard Time.

"**Affected Participant**" means a Framework Participant that is experiencing a Disabling Event which prevents that Framework Participant from sending HVCS payments in the normal way.

"**Agent**" means a participant in the payment chain that executes the movement of funds between, either the Framework Participant of the payer, or payee, or an intermediary Framework Participant.

"**AIF**" means automated information facility, which means the service provided within RITS for the initiation and monitoring of SWIFT message based commands, enquiries and unsolicited advices.

"**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.

"**Assisted Transaction**" means a transaction entered into RITS by the RBA on behalf of the Framework Participant, subject to the appropriate authorisation and in accordance with the RITS Regulations.

"**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 set out in Part 7.

Back-up Tier means either of the two tiers of back-up applicable to a Framework Participant, as determined from time to time in accordance with Part 7. A Framework Participant's Back-up Tier sets the back-up requirements with which that member must comply.

"**BAH**" means business application header, which means a header that is combined with another MX message to form a Business Message. It is defined by the ISO 20022 community in the XML schema head.001.001.xx.

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

"**BIC**" means business identifier code, which means an international standard for identification of institutions within the financial services industry. BICs consist of:

(a) institution code consisting of 4 alphabetic characters

(b) country code consisting of 2 alphabetic characters

(c) location code consisting of 2 alpha-numeric characters and

(d) optionally, a branch code consisting of 3 alpha-numeric characters, also known as the Branch Identifier.

Parts (a), (b) and (c) together constitute an 8-character BIC, also referred to as a BIC8, and with the addition of part (d) an 11-character BIC, also referred to as a BIC11.

"**Business Officer**" means a person who has the authority to instruct SWIFT to change the SWIFT Messaging Service mode.

"**Business Message**" means the ISO 20022 format message sent between Framework Participants.

"**BIC/BSB Directory**" means the HVCS directory in which the BIC/BSB particulars for Framework Participants are recorded and published.

"**BSB Number**" means a six-digit number that identifies banks and branches across Australia. In relation to a Framework Participant, it means the BSB number assigned to it by the Company.

"**Business Day**" means a day on which RITS is operating to process payments.

"**Case**" means an investigation into a payment or payments conducted within an HVCS CUG.

"**CBPR+**" means Cross-Border Payments and Reporting Plus, which means a SWIFT and PMPG working group responsible for developing ISO 20022 global usage guidelines for cross-border payments.

"**CCB**" means Change Control Board, which means a body comprised of industry experts charged with the maintenance of HVCS MUGs.

"**Certification Test Plan**" means the test plan, incorporating test scripts, produced by the Company for the purpose of obtaining System Certification, to ensure that a Framework Participant's SCI has the correct PDS configuration loaded and can successfully interact with SWIFT Messaging Service.

"**CEST**" means Central European Summer Time.

"**CET**" means Central European Time.

"**CLS**" means continuous linked settlements, which means a global initiative to reduce foreign exchange settlement risk by settling both legs of foreign exchange transactions simultaneously.

"**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."**Coexistence Period**" [Deleted][1]

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

"**Core Business Hours**" means from 9:15am to:

(a) 5:15pm for Non-Eligible Payments; and

(b) 6.30pm / 7.30pm / 8.30pm (as applicable) for Eligible Payments, each Business Day.

"**Core PPS**" means the specific hardware and software that is normally used by Framework Participants to generate or process the bulk of their HVCS messages, by value, for high value payments. This would include, for example, systems required for sending correspondent banking and financial markets transactions.

"**Corporations Law**" means the Corporations Act 2001 (Cth).

"**Crisis Communication Plan**" means the documented framework to enable members of the Company to communicate with each other during a major disruption to any of the payments clearing, settlement or infrastructure systems that fall under the remit of the Company.

"**CSI**" means central SWIFT interface, which means the RITS interface to the SWIFT Messaging Service.

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

"Cyber Fraud Event" means any actual or suspected unauthorised or fraudulent payment that:

(a) arises as a result of a cyber security breach in the Framework Participant's own control environment: and

(b) is known or suspected to have been dispatched to another Framework Participant through the SWIFT PDS CUG.

"**Daily Settlement Session**" means the session running from 9:15am to 4:30pm as set out in the RITS Regulations.

"**Disabling Event"** means:

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

[1] Deleted effective 23/9/24, version 4 r&p 001.24

(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.

"**DN means**" distinguished name, which means a unique identifier (including the BIC) used for message routing in the SWIFT network.

"**Eligible Payment**" means a Payment where both the Sender and Receiver have agreed to operate in the Evening Settlement Session.

"**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.

"**ESA**" means exchange settlement account, which means an account maintained by a Framework Participant with the RBA.

"**ESR**" means exchange settlement rate, which means the interest rate payable by the RBA on overnight credit balances of exchange settlement accounts.

"**Evening Settlement Session**" means the session running from close of Interim Session to 10:00pm as set out in the RITS Regulations.

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

"**Exchange Summary Form**" means a summary document substantially in the format prescribed by the Reserve Bank of Australia, and available on the Company's extranet.

"**FileAct**" means an automated SWIFT messaging service designed to enable customers to exchange files. The service supports both interactive and store-and-forward modes. It is particularly suited for the exchange of large volumes of data.

"**FINplus**" means a SWIFT Messaging Service which enables financial institutions to exchange the ISO 20022 messages for securities and payments. Its uses include cross-border payments in the CBPR+ format.

"**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.

"**FTM**" means Failure to Match, which means a mis-match of settlement amounts provided by Framework Participants to the RBA when settlement is deferred due to a Disabling Event.

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

"**gpi**" means global payment initiative which means a SWIFT initiative to facilitate end-to-end tracking and reporting of payment status.

"**HSM**" means hardware security module, which means a hardened, tamper-resistant device used for safe storage, generation and management of digital keys.

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

"**HVCS Bilateral Clearing Form**" in relation to a Participant Fallback Period, means a form in the format prescribed by the Company that an Affected Participant uses to send HVCS payments to another Framework Participant.

"**HVCS Contingency Instructions**" means the instructions set out in Annexure J.

"**HVCS Exchange Figures Advice**" in relation to a HVCS Fallback Period, means a summary document (provisional or final), issued by and in a format prescribed by the RBA, showing the net obligations between a Framework Participant and the other Framework Participants, as calculated by the RBA using data received from Framework Participants in the HVCS Exchange Summary Form.

"**HVCS Fallback Period**" means a period declared by the Chief Executive Officer to be a HVCS Fallback Period under clause 9.21(d) to authorise the use of the HVCS Fallback Solution as the method for clearing and settlement of HVCS payments during a RITS Outage.

"**HVCS Fallback Solution**" means the method used for clearing and settlement of HVCS payments during a HVCS Fallback Period that is outlined in the HVCS Contingency Instructions.

"**HVPS+**" means High Value Payments Plus, a self-governed group, comprised of high value financial market infrastructures from around the world, that maintains a template ISO 20022 message collection.[2] .

"**IBAN**" means International Bank Account Number, which means a standard code used to identify an overseas bank account number.

"**IFTI**" means International Funds Transfer Instruction.

"**IMSC**" means Industry Migration Steering Committee.

"**Instructing Agent**" means a party that instructs the next party in the chain to carry out the (set of) instruction(s).

"**Instructed Agent**" means an agent that is instructed by the previous party in the chain to carry out the (set of) instruction(s).

"**InterAct**" means a global financial messaging service used by the SWIFTNet platform.

[2] Amended effective 23/9/24, version 4 r&p 001.24

"**Interim Session**" means the session running from 5:15pm to approximately 5:16pm as set out in the RITS Regulations.

"I**ntermediary Agent**" means an agent between the debtor's and creditor's agent.

"**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.

"**ISO**" means International Standards Organisation.

"**ISO 20022**" means a message standard for financial markets developed and maintained by ISO.

"**ISO 20022 CUG**" means the closed user group used to send and receive MX format HVCS messages.

"**LEI**" means legal entity identifier, which means a 20-character alpha-numeric code allocated to organisations using the ISO 17442 format. The code is designed to uniquely identify legally distinct entities that engage in financial transactions.

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

"**Morning Settlement Session**" means the session running from 7:30am to 8:45am as set out in the RITS Regulations.

"**MT**" means the SWIFT proprietary message format.

"**MT CUG**" is the closed user group used to send and receive MT format HVCS messages.

"**MUGs**" means "Message Usage Guidelines", which means the guidelines available to the 'HVCS Community' on the SWIFT MyStandards platform.

"**MX**" means the suite of SWIFT message types defined by an ISO 20022 XML schema. "**MX Readiness Register**" [Deleted][3]

"**NAK**" means negative acknowledgment, which 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 Clearing System Obligations Advice**" in relation to a HVCS Fallback Period, means a summary document, issued by and in a format prescribed by the RBA that shows a Framework Participant's net obligation in the multilateral contingency batch for settlement in RITS, including clearing system interest.

"**Non-Eligible Payment**" means all Payments other than Eligible Payments.

"**Participant Fallback Period**" means a period declared by the Chief Executive Officer to be a Participant Fallback Period under clause 9.21(d) to authorise the use of the Participant

[3] Deleted effective 23/9/24, version 4 r&p 001.24

Fallback Solution as the method for clearing and settlement of HVCS payments during a Participant Outage.

"**Participant Fallback Solution**" means the method for clearing and settlement of HVCS payments during a Participant Fallback Period that is outlined in the Contingency Instructions.

"**Participant Outage**" means a period during which a Framework Participant experiences a Disabling Event which prevents that Framework Participant from sending HVCS payments in the normal way.

"**Payment**" means, in relation to a SWIFT PDS, a payment submitted via that SWIFT PDS for settlement in RITS.

"**Pilot DN**" means the distinguished name used in the pilot (pre-production/test) Closed User Group.

"**PKI**" means Public Key Infrastructure, which means information exchanged between parties to facilitate the transmission of encrypted data.

"**PMPG**" means Payments Market Practice Group, which means an international forum, facilitated by SWIFT, that assists industry participants formulate better market practices, including the recommended use of standards. Further details on the group can be found at: https://www.swift.com/about-us/community/swift-advisory-groups/payments-marketpractice-group.

"**PPS**" means Payments Processor System, which means hardware and software used to generate or process HVCS messages.

"**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 Part 7.

"**RBA**" means Reserve Bank of Australia.

"**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.

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

"**Reports Session**" means the session running from 10:00pm to 10:30pm or such later time as the RBA may prescribe from time to time.

"**RITS**" means the settlement system established and operated by the RBA for RTGS and includes the CSI. For the avoidance of doubt, references to RITS include that system when operating to effect settlement of Payments on a RTGS basis and when otherwise operating to effect settlement of payments on a deferred net settlement basis.

RITS Allocation balance has the meaning given in the RITS Regulations.

"**RITS Cash Transfer** or **Cash Transfer**" means the transfer of funds between ESAs undertaken using functionality provided by the RBA in the RITS User Interface and in accordance with the RITS Regulations.

"**RITS Outage**" means a period during which the central site (RITS or CSI) is experiencing a Disabling Event that prevents RITS or CSI, as applicable, from effecting settlement of HVCS payments in the normal way.

"**RITS Regulations**" means the regulations for RITS published from time to time by the RBA.

"**RITS UI**" means the user interface made available by the RBA through which RITS Members or the RBA may input, view and manage transactions; perform administration activities; view and download reports; and perform other ancillary actions within RITS, in accordance with the RITS Regulations.

"**RTGS**" means real time gross settlement, which 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.

"**RMA**" means relationship management application, which means a filter that manages which message types are permitted to be exchanged between users of a SWIFT service.

"**Schema**" means a logical collection of database objects which define the messaging format.

"**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.

"**Settlement Close Session**" means the session running from 4:30pm to 5:15pm as set out in the RITS Regulations.

"**Settlement Day**" means a day on which Payments are processed in RITS as specified in, or in accordance with, the RITS Regulations.

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

"**SLS**" means Secure Login Select, which is an encryption security protocol.

"**SWIFT**" means Society For Worldwide Interbank Financial Telecommunication.

"**SCI**" means SWIFT Customer Interface, which means the systems and software supporting the messaging interface to the SWIFT Messaging Service.

"**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.

"SWIFT Customer Security Mandatory Controls Non-Compliance Form" means the form set out in Annexure 3.

"**SWIFT FIN (FIN)**" means the SWIFT messaging service that enables the exchange of MT messages.

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

"**SWIFT Knowledge Centre**" means the online repository of reference documentation provided by SWIFT.

"**SWIFT Messaging Service**" means a service provided by SWIFT. In respect of the messaging services provided to Framework Participants (including SWIFT FIN-Copy Service and/or SWIFTNet Copy Service) the service is provided pursuant to a SWIFT Service Agreement.

"**SWIFT MyStandards**" means the repository where ISO 20022 message specifications and other related information are maintained and published by the Company.

"**SWIFT MyStandards Readiness Portal**" means the testing portal that allows Framework Participants to test their messages against the formal rules (not textual rules) as set out in the HVCS MUGs.

"**SWIFTNet Header**" means part of the envelope of a SWIFT ISO 20022 message which contains elements to address the message to the correct SWIFTNet service or CUG. These include *RequestControl, RequestResponse, ExchangeRequest, Request,* and *RequestHeader*.

"**SWIFTNet Copy Service**" means the copy service provide by SWIFT, under normal circumstances operating in Y-Copy mode, but which can be switched to T-Copy mode in the event of a RITS Outage.

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

"**SWIFT PDS**" means a SWIFT Messaging Service, operating, under normal circumstances, in Y-Copy mode, configured with Framework Participants' SCIs to meet the processing requirements of the HVCS, together with any ancillary SWIFT services provided in connection with the applicable SWIFT Messaging Service.

"**SWIFT PDS CUG**" is the group of Framework Participants admitted to use the SWIFT PDS (either through the MT CUG and/or the ISO 20022 CUG (as applicable)) to send and receive payments.

"**SWIFT PDS Log**" means the record to be maintained by Framework Participants in accordance with clause 4.8 of all system outages, changes to the SWIFT PDS configuration and system test details.

"**SWIFT PDS Queue**" means a queue in the SWIFTNet.

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

"**SWIFT Regional Account Manager**" means the person designated as such from time to time by the Chief Executive Officer.

"**SWIFT Secure Channel**" means an online application provided by SWIFT, through which a Business Officer can instruct SWIFT to change to the SWIFT Messaging Service mode.

"**SWIFT Service Agreement**" means (as applicable):

(a) the agreement effective 16 December 1996 entitled Agreement between the Company and SWIFT for FIN-Copy Service Administration, pursuant to which SWIFT provides its SWIFT FIN Copy Service to Framework Participants; and/or

(b) any other agreement between the Company and SWIFT entered into from time to time pursuant to which SWIFT provides SWIFT Messaging Services to Framework Participants.

"**SWIFT T-Copy** or **T-Copy**" means a copying mode of the SWIFTNet service where payment messages are sent directly to the intended recipient with a copy sent to RITS without authorisation.

"**SWIFT Y-Copy** or **Y-Copy**" means a message flow where parts of payment messages are copied to RITS for settlement execution before the whole instruction is delivered to the intended recipient for clearing.

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

"**System Administrator**" means the person appointed by the RBA to supervise operation of RITS.

"**System Certification**" means 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 SWIFT PDS.

"**System Certification Checklist**" means a checklist in the form of Annexure A 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 7.15 by the Management Committee to a Framework Participant which has successfully completed the process for System Certification.

"**System Queue**" means a queue held by RITS in which each Payment (other than a Warehoused Payment) is held pending processing in RITS prior to settlement.

"**Total National Transaction Value**" means, in respect of a SWIFT PDS, the aggregate value of all Payments sent and received by all Framework Participants using that SWIFT PDS. This aggregate value is determined using the statistical data collected for the purposes of and in accordance with clause 7.10(a).

"**TPP**" means third party providers, which means a provider of relevant services to a Framework Participant, including Infrastructure as a Service (IaaS) cloud hosted services.

"**Ultimate Creditor**" means the ultimate party to which an amount of money is due.

"**Ultimate Debtor**" means the ultimate party that owes an amount of money to the (ultimate) creditor, such as the buyer of services or goods.

"**Universal Confirmation**" means a confirmation sent by the beneficiary's bank that funds have reached the beneficiary's account.

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

"**Warehoused Payments**" means Future Dated Payments received by RITS and held pending the settlement date when the payments are placed on the System Queue for normal processing.

"**XML**" means Extensible Markup Language.

"**Yearly Audit Compliance Certificate**" means a certificate in the form of that in Annexure B.

"**Year**" means a calendar year.

1.2 Interpretation

In these Procedures:

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

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

(c) 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;

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

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

(f) Words defined in the MUGs have, unless the contrary intention appears, the same meaning in these Procedures.

(g) Terms that are both Italicised and capitalised but otherwise remain undefined within the Regulations or Procedures may generally either refer to:

(h) documents published by a third party such as SWIFT or the RBA; or

(i) names of ISO 20022 message types or data elements within those messages, as set out in the HVCS MUGs.

(j) These Procedures have been determined by the Management Committee and take effect on the date specified by the Chief Executive Officer.

(k) Headings are inserted for convenience and do not affect the interpretation of these Procedures.

1.3 Inconsistency with Articles or Regulations

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

(b) If a provision of these Procedures is inconsistent with a provision of the Regulations, the provision of the Regulations prevails.

1.4 Governing Law

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

1.5 Copyright

The next page is Part 2

PART 2 EFFECT

(a) These Procedures have the effect set out in Part 2 of the Regulations.

(b) 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 and associated messages sent and received electronically using the SWIFT PDS.

(c) The HVCS Procedures consist of two volumes:

(i) Volume 1, which applies to participation in the HVCS MT CUG; and

(ii) This volume 2, which applies to participation in the HVCS ISO 20022 CUG for the processing of MX messages.[4]

(d) Participation in the HVCS requires participation in both CUGs, and therefore adherence to both volumes of the Procedures. Neither volume can be relied upon in isolation. There is no hierarchy or precedence between the two volumes. Volume 1 applies to the processing of MT format messages. Volume 2 applies to the processing of MX messages. Both volumes contain a Part 9 relating to contingency processing and associated contingency instructions in an annexure to each volume. Both sets of procedures and instructions must be considered together.[5]

The next page is Part 3

[4] Amended effective 23/9/24, version 4 r&p 001.24
[5] Amended effective 23/9/24, version 4 r&p 001.24

PART 3 PROCEDURES AND AMENDMENT

3.1 Conduct of Clearings

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.

3.2 Amendments

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

(b) Each Framework Participant must notify the Company of any changes to its contact points as specified in the Company extranet, which will be maintained by the Company.

3.3 Inconsistency with Other Applicable Rules and RITS Regulations

(a) 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 RBA in relation to RITS. Those requirements of SWIFT or the RBA might change from time to time.

(b) Subject to this clause 3.3(b), 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:

(i) deals with the same subject as any provision of the "SWIFT User Handbook";

(ii) 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

(iii) 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".

(c) 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.

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

The next page is Part 4

PART 4 GENERAL OPERATIONAL REQUIREMENTS

4.1 RITS Operating Day

(a) The RITS operating day is made up of four distinct operating sessions plus three closed sessions to enable completion of the 9am Settlement, preparation for the Evening Settlement Session and overnight processing. The usual times for the sessions and the processing arrangements are set out in the RITS Regulations and summarised below, but the RBA may advise other times on any given day. Framework Participants must refer to the RITS Regulations for up to date information on the RITS operating day.

(i) Morning Settlement Session

Framework Participants may use the Morning Settlement Session to fund their 9am 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.

(ii) 9am Settlement Session

Only RITS processing associated with the 9am Settlement will be undertaken during the 9am Settlement Session.

(iii) Daily Settlement Session

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.

(iv) Settlement Close Session

(A) 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.

(B) Framework Participants must use reasonable endeavours to agree to operate in the Evening Settlement Session to settle Payments remaining on the System Queue following closure of the Daily Settlement Session. This will assist all Framework Participants in managing their end of day liquidity requirements.

(C) 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.

(v) Interim Session

No transaction processing occurs during the Interim Session. This session is designed to allow those Framework Participants, who have Non-Eligible Payments to obtain end of day reports and finalise their day's work.

(vi) Evening Settlement Session

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 4.3(b)). Eligible Payments remaining on the System Queue at 6.30pm / 7.30pm / 8.30pm will be rejected.

(vii) Reports Session

(A) 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.

(B) 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.

4.2 SWIFT PDS OPERATING DAY

(a) SWIFT PDS operating hours for the sending of Payments are:

(i) 9.15am to 4.30pm Monday to Friday for the exchange of all applicable message types; and

(ii) until 6.05pm / 7.05pm / 8.05pm* (refer clause 4.3(b)) for the exchange of FI To FI Credit Transfers and associated messages for Eligible Payments.

(iii) Framework Participants may initiate payments, for same day value, at any time during the SWIFT PDS operating hours as set out in the RITS Regulations.

(iv) Following closure of the SWIFT PDS for the day, RITS will continue to accept same day value payments provided:

(A) SWIFT has sent an ACK for that pacs.008 payment prior to 4.30pm;

(B) SWIFT has sent an ACK for that pacs.009 (CORE/COV) payment prior to 4.30pm for Non-Eligible Payments or prior to 6.05pm / 7.05pm / 8.05pm*(refer clause 4.3(b)) for Eligible Payments; and

(C) the payment is received at System Queue prior to 4.30pm for Non-Eligible Payments and prior to 6.05pm /7.05pm/ 8.05pm* (refer clause 4.3(b)) for Eligible Payments.[6]

(b) All payments on the System 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.

(c) Eligible Payments remaining on the System Queue at 6.30pm / 7.30pm / 8.30pm* (refer clause 4.3(b)) will be rejected.

(d) Future Dated Payments initiated on any particular Business Day after closure of the SWIFT PDS will be held on the SWIFT PDS Queue pending dispatch to RITS on the next Business Day.

4.3 Extension of Normal Operating Hours

(a) RITS operating hours may be extended or varied by the RBA 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.

(b) Note in relation to processing times:

(i) Certain operational times are determined with reference to CET and CEST and therefore will vary throughout the year.

(ii) As a guide CEST commences at the end of March and concludes at the end of October. AEDT usually commences at the beginning of October and concludes at the start of April. However, the relevant commencement and conclusion dates do not always coincide.

(iii) The following table may assist Framework Participants in aligning processing times for summer time and normal time across the two time zones.

(A) 10.00am CET = 8.00pm AEDT

(B) 10.00am CEST = 6.00pm AEST

(C) 10.00am CEST = 7.00pm AEDT

(D) 10.00am CET = 7.00pm AEST

(iv) The closure times for the Evening Settlement Session may be varied by the RBA in consultation with the Company. 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.

[6] Amended effective 6/6/23, version 2 r&p 001.23

(v) The RBA or the System Administrator will, where practicable, notify HVCS Framework Participants of any such variations in advance of the day(s) that those variations apply to.

4.4 SCI Start Up Requirement

(a) Framework Participants must be logged on to SWIFT PDS prior to 9.15am on each Business Day and remain logged on for the Core Business Hours.

(b) If a Framework Participant:

(i) is unable to log its SCI on to SWIFT PDS for commencement of the Daily Settlement Session;

(ii) experiences any technical or operational problem with its SCI during the then current Business Day; or

(iii) experiences any technical problems with its Core PPS during the then current Business Day, which prevents it from processing payments, the Framework Participant must advise details of the outage to the System Administrator as soon as possible, but no later than 30 minutes after that Framework Participant first became aware of the problem.

(c) Where it is considered the outage will be protracted the System Administrator will advise Framework Participants in accordance with PART 9.

(d) Where a Framework Participant has advised details of a system outage in accordance with clause 4.4(c) 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 4.4(d), the System Administrator will immediately advise Framework Participants of the changed circumstances if they have been notified of the system outage.

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

(f) Framework Participants experiencing difficulties with their Core PPS, rather than their SCI, must ensure that the SCI remains logged on to SWIFT PDS for the entire Business Day to allow for the receipt of inward payments.

(g) Full details of Contingency procedures requirements are set out in Part 9 of these Procedures.

4.5 SCI Close Down

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”.

4.6 Holiday Arrangements

(a) The SWIFT PDS will be open for normal operations on any day on which RITS is operating.

(b) 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.

(c) 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.

4.7 SWIFT PDS BIC/BSB Data

(a) 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".

(b) The "HVCS BIC/BSB Directory" will list all SWIFT PDS BIC/BSB links both numerically, by BSB number, and alphabetically in Framework Participant order.

(c) If a Framework Participant operates multiple SWIFT PDS BICs, that member must advise the Company of details of each BSB linked to each BIC.

(d) 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 publication of the updated BIC/BSB Directory.

4.8 SWIFT PDS Log

(a) Framework Participants must maintain a SWIFT PDS Log in which they will record details of all:

(i) system outages and the time required to re-establish live operations (clause 4.4(d));

(ii) alterations to their Primary and Backup Computer Site system configurations (see PART 7);

(iii) the date, time, duration and results of Backup Computer Site testing (see PART 7); and

(iv) the date, time, duration, and percentages of all reportable instances of degraded SCI performance (clause 7.14) and the cause and remedy (if known).

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

4.9 Rules Governing Compensation Claims

(a) 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.

(b) 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. 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.

4.10 Disputes Relating to Compensation Claims

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.

4.11 Receiver Unable to Apply Payment

(a) This clause 4.11 is subject to the procedures set out in clause 4.15 to 4.21 and applies where the Receiver is unable to apply an inward payment due to incorrect or incomplete beneficiary information. In such cases payment must be returned:

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

(ii) 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 4.11(b)).

(b) Where the Receiver is unable under clause 4.11(a) to return a payment on the day of receipt of it, the Sender is entitled to compensation in accordance with the Inter-Organisation Compensation Rules for the Receiver's use of the funds.

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

(i) Any apparent breach of this clause 4.11, should immediately be brought to the attention of the Framework Participant concerned, so that corrective action can be taken by that Framework Participant.

(ii) Continual breaches of this clause 4.11 by the same Framework Participant must be reported to the Management Committee.

(iii) (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.)

4.12 Incorrectly Applied Items

(a) This clause 4.12 must be read in conjunction with the procedures set out in clauses 4.15 to 4.21.

(b) 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 4.11(b)), 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.

(c) 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. 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.

(d) If the Sender requests the Receiver to endeavour to reverse a payment in accordance with clause 4.12(b) 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.

4.13 Processing by Account Number Only

(a) This clause 4.13 must be read in conjunction with the procedures set out in clauses 4.15 to 4.21.

(b) 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 of 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

4.13 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.

Notes:

(i) For the purpose of this clause 4.13, 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.

(ii) 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.

4.14 Requests for Back Valuation and Forward Valuation of Payments

(a) This clause 4.14 must be read in conjunction with the procedures set out in clauses 4.15 to 4.21.

(b) Where a payment is received after its due date because the Sender dispatched it late, the Sender may request the Receiver to back value the payment. On receipt of a request under this clause 4.14 to back value a payment, the Receiver must back value that payment, subject to refusal justifiable on legally sustainable grounds.

(c) Where a payment is back valued under this clause4.14, the Receiver is entitled to compensation from the Sender.

(d) Where a payment is received before its due date because the Sender dispatched it early, the Sender may request the Receiver to forward value the payment. On receipt of a request under this this clause 4.14 to forward value a payment, the Receiver must forward value that payment, subject to refusal justifiable on legally sustainable grounds.

(e) Where a payment is forward valued under this clause 4.14, the Sender is entitled to compensation from the Receiver.

4.15 Case Management

(a) This clause 4.15 applies to domestic payment investigations and returns conducted within the ISO 20022 CUG (including the domestic leg of cross-border transactions). Separate rules, as outlined by CBPR+, will apply to cross-border scenarios. If an investigation extends cross-border, it should generally be treated as a separate investigation, with the domestic and cross-border components treated as separate Cases.

(b) A ‘Case’ is defined as follows:

(i) A Case is created each time an exception and investigation process is needed.

(ii) A Case is a file that records the progress of the investigation. This file can be paper-based (a physical folder) or electronic (a database table).

(iii) A party creates and organises a Case file in its preferred way through an internal Case management process supported by a variety of tools/applications.

(c) The table below summarises the messages used to conduct exception and investigation processing.

Message Type	Payment Return	Exceptions & Investigations (E&I)
camt.056 – *FI to FI Payment Cancellation Request*	Mandatory message for requesting a payment cancellation. Conveys the mandatory element – *Case/Identification <Case /Id>* which is designated a *Primary Case ID*.	Must be used in an investigation if one party initiates a request for a payment cancellation.
camt.029 – *Resolution of Investigation*	Responds to camt.056 to convey status (i.e. *Accept*, *Reject* or *Pending*). Must convey the *Primary Case ID* of the underlying camt.056 in Resolved Case/Identification <RslvdCase/Id>. Should be used to convey the *Secondary Case ID*, if assigned, in *Cancellation Status Reason Information /Additional Information <CxlStsRsnInf/AddtlInf>*. Must be used to resolve a camt.056.	Where a request for payment cancellation has been initiated, a resolution of investigation must be used to communicate the outcome of the request for cancellation.
MTn99 – *Free Format Message**	Used if optional communication is required between parties.	Used to initiate and respond to general enquiries and requests for investigation. May optionally be used to convey *Primary Case ID* in *Tag 21 Related Reference*, and *Secondary Case ID* in *Tag 79 Narrative.* May optionally be used to convey investigation resolution.

* Outside of the HVCS MT CUG, Framework Participants are also free to use other message types as necessary, using the formatting rules that apply to those message type, for example MTn92/95/96.[7]

[7] Amended effective 23/9/24, version 4 r&p 001.24

(d) All camt.*xxx E&I* messages relating to an HVCS payment, must be conducted within the SWIFT PDS CUG, except where:

(i) Both parties to the investigation are also members of FINplus and agree a preference to use it instead;

(ii) An offshore bank requests a payment return using a camt.056 directly to the recipient bank, bypassing the Australian intermediary; or

(iii) Both parties to the investigation are also gpi banks and agree a preference to carry out the investigation through the gpi tracker.

4.16 Investigation Case Lifecycle

(a) The lifecycle of an HVCS Case, from the opening of an investigation to the closure of a Case, is described in the table below.

Question	Message Type	Description
When can a primary Case start?	A primary Case may start when a party sends either: • camt.056 *Request for Payment Cancellation*; or • MT199 query or investigation message.	• The **camt.056** message is: o Used to request the cancellation of a payment, for example in the case of a mistaken payment; o May be used to open a new Case (where there is no existing Case being referenced) or an existing Case (as part of an ongoing investigation). • The **MT199** message: o Is a free form message which is used to initiate or respond to general queries and investigations; [8] o Can be used to open a new Case.
When does a primary Case close?	A Case can be closed by either party when it makes sense to close a Case, without specific messaging from the other party. Alternatively, a Case can close when a party sends any of: • camt.029 Resolution of Investigation; or • MT199 with free-form messaging to notify Case closure.	Either party to a general investigation may close the Case without advising the other party: • The **camt.029** message: o Is used to either accept, reject, or provide a pending status for a Request for Payment Cancellation (camt.056); and o It may be used to signify Case closure (when the *Request for Payment Cancellation* is accepted or rejected). • The **MT199** message: o May be used to convey Case closure; o In instances where a MT199 does not require a response, it effectively both opens and closes the referenced Case.

(b) Sometimes, a Case may be closed prematurely by either party (either with or without specific messaging). To continue managing the investigation efficiently, a Case

[8] Amended effective 23/9/24, version 4 r&p 001.24

should be reopened under the same primary Case identification number wherever possible, rather than creating a new Case. There should only be one primary Case identification number associated with a single underlying payment (as identified by the UETR), recognising that two or more Cases can be conducted on one message for different purposes – for example, when a fraud team and a payments team are both working on a payment and have different Case references.

(c) If a party assigns a secondary Case identification number, it should be conveyed to the originating party via either:

(i) A camt.029 in Cancellation Status Reason Information /Additional Information <CxlStsRsnInf/AddtlInf>; or

(ii) An MT199 in Tag 21 Narrative.

4.17 Service Levels for Domestic E&I Messages

The purpose of the service levels is to create efficiency in handling *E&I* messages and reduce the need for parties to follow up outstanding requests. Service levels will only be applied to messaging conducted within the ISO 20022 CUG and not to messaging in the MT CUG, including MTn99 messaging which is used in conjunction with camt.xxx messages.

4.18 Service Level for Response [9]

(a) Upon receipt of a camt.056, the Framework Participant must respond by the end of the next Business Day in the form of either:

(i) A camt.029 to signify request rejection or to provide a pending status, or

(ii) A pacs.004 (or pacs.008 / pacs.009 (CORE/COV) together with a camt.029 to signify completion of the request.

4.19 Service Level for Investigation Resolution

(a) Framework Participants must endeavour to complete simple investigations within one day. The service level to complete all investigations is within 10 business days on which RITS is operating, accepting that:

(i) some returns have specific service levels attached e.g. mistaken payments follow the ePayments Code and duplicate payments arising from a technical error; and

(ii) some fraud-related investigation activities may take longer, and the service levels may not be met.

(iii) Investigation resolution is reached when both parties agree on a course of action, not necessarily when all of those actions have been completed. For example, parties may agree a payment plan with a customer to repay in

[9] Amended effective 23/9/24, version 4 r&p 001.24

instalments. In this instance, resolution has been reached, even though the payments may take some months to be completed.

4.20 Returning a Payment [10]

(a) Payments made in the ISO 20022 CUG (pacs.008 and pacs.009 CORE/COV) must be returned with a pacs.004. [11]

(b) Framework Participants should include all available transaction reference identifiers in the return message to allow the recipient of the return to link the two messages back together, including the *Transaction Identification*, *Instruction Identification* and UETR.

(c) A table can be found in Annexure F to help in the population of mandatory pacs.004 elements from the original payment that is being returned.[12]

4.21 MX Readiness Register [Deleted][13]

The next page is Part 5

[10] Amended effective 23/9/24, version 4 r&p 001.24
[11] Amended effective 23/9/24, version 4 r&p 001.24
[12] Amended effective 23/9/24, version 4 r&p 001.24
[13] Deleted effective 23/9/24, version 4 r&p 001.24

PART 5 SWIFT PDS CLOSED USER GROUP

5.1 Overview

(a) The USO 20022 CUG uses the facilities to the SWIFTNET Copy Service over InterAct and MUGs tailored to meet the needs of the Australian domestic HVCS. 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, as well as other applicable security standards.

(b) Each Applicant proposing to use the SWIFT PDS which is not a SWIFT User, should contact SWIFT to discuss SWIFT connectivity requirements by contacting SWIFT Asia-Pacific Commercial Services team via swift.com. The Applicant will be assigned to a SWIFT account manager for in-depth discussions. SWIFT advises that Applicants proposing to use the SWIFT PDS should allow at least 6 months to complete the SWIFT membership process and implement SWIFT connectivity.

(c) Each Applicant proposing to use the SWIFT PDS which is not a RITS member and ESA holder, must contact the RBA to discuss membership requirements, including the establishment of an ESA. Participation in the HVCS requires RITS membership and the use of an ESA.

5.2 ISO 20022 CUGs

(a) There are two ISO 20022 CUGs: a pre-production closed user group (i.e. test or pilot) and production. A Framework Participant must join both.

(b) All HVCS pacs.xxx and camt.xxx messages are transacted on the ISO 20022 CUG, while system messages (xcop.001 and xsys.xxx) and *Customer-to-FI/FI-to-Customer* messages are transacted outside of the ISO 20022 CUG.

5.3 RMA Requirements

The RMA is not used within the ISO 20022 CUG. Framework Participants may continue to require an RMA to facilitate message exchange between local Framework Participants outside of the ISO 20022 CUG.

5.4 Concurrent Membership of MT CUG and ISO 20022 CUG[14]

(a) All HVCS Framework Participants must join both the production and pre-production (pilot) ISO 20022 CUG, as described in 5.2.

(b) At the same time, Framework Participants must also remain in the MT CUG.[15]

5.5 SWIFT PDS Closed User Group Management

(a) The SWIFT PDS CUG is administered by the Company. The Company is responsible for certification as set out in Part 7, the daily operation of the SWIFT

[14] Amended effective 23/9/24, version 4 r&p 001.24
[15] Amended effective 23/9/24, version 4 r&p 001.24

PDS CUG and the maintenance and implementation of the HVCS Regulations and Procedures applicable to the SWIFT PDS CUG.

(b) Applicants should contact the Secretary concerning requirements for HVCS membership and the requirements in relation to use of the SWIFT PDS.

5.6 SWIFT PDS CUG Membership Application – General

Applicants proposing to use the SWIFT PDS are required to complete the applicable SWIFT e-form for SWIFT PDS CUG subscription for the pilot and/or live service (as the case may be) and submit completed forms online through SWIFT.com.

5.7 SWIFT PDS CUG Membership Application for Test and Training

(a) 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 by SWIFT of the application and inclusion of the Applicant's details in the SWIFT PDS CUG records.

(b) Once the Company approves the subscription, SWIFT will then complete the necessary provisioning.

(c) Details of this process are provided by the Company when on-boarding new Framework Participants, including details of how to provide pilot and production DNs during the subscription process.

5.8 SWIFT PDS CUG Membership Application for Live Operations

(a) As part of the System Certification process set out in clause 7.15, each Applicant must complete the applicable SWIFT e-form for SWIFT PDS CUG subscription for live operations, submit it via SWIFT.com and forward the completed System Certification Checklist to the Company. Details of this process are provided by the Company when on-boarding new Framework Participants.

(b) Where the Applicant's application for System Certification is successful the Company will, following Management Committee's approval in accordance with Regulation 5.5, approve the subscription. SWIFT will then complete the necessary provisioning.

(c) The Secretary will, in accordance with Regulation 5.7, advise the Applicant of the date on which the Applicant is accepted as a Framework Participant and may commence participation in SWIFT PDS.

5.9 Amendment of Framework Participant SWIFT PDS CUG Details

Any Framework Participant wishing to amend its SWIFT PDS CUG details must complete the applicable e-form through SWIFT.com for approval by the Company and subsequent processing by SWIFT.

5.10 HVCS Suspension/Withdrawal of a Framework Participant

(a) Where a Framework Participant's membership of HVCS is terminated pursuant to Regulation 5.17 or is suspended pursuant to Regulation 5.10, this will result in

termination of the Framework Participant's membership to the SWIFT PDS CUG and require reapplication to the SWIFT PDS CUG membership. The Company will immediately advise SWIFT of the change to the SWIFT PDS CUG membership.

(b) SWIFT will confirm receipt of the request with a further advice confirming removal of applicant data from the SWIFT PDS CUG, as applicable.

5.11 HVCS Framework Participant Re-entry

(a) Where the Company revokes a Framework Participant's suspension pursuant to Regulation 5.16, it must immediately advise SWIFT of the reinstatement of the member.

(b) SWIFT will confirm receipt of the request, with a further advice confirming successful implementation of applicant data and such Framework Participant may reapply to the SWIFT PDS CUG.

5.12 Bank Identifier Code (BIC) and Distinguished Name (DN)

(a) Framework Participants must have a SWIFT BIC that is published in both the "SWIFTNet Directory" and the BIC/BSB Directory maintained by the Company. Framework Participants can define multiple BICs for use within the SWIFT PDS.

(b) For the HVCS production service, DNs must consist of 3 levels. The first level (the root level) is always o=swift. The second level is the published BIC8 and the third level a 3-character branch code (or xxx if no branch code is specified). Hence, Participants will always be able to derive the production DNs of other Participants from the BIC register which is maintained by the Company. More details on DN structure, including examples, are contained in part 9 of Annexure F.

5.13 Warehoused Payments

(a) Framework Participants may enter any payment (as a Future Dated Payment) into the SWIFT PDS System. RITS determines the value date from the "Value Date" contained within the *Interbank Settlement Date* element of the payment message. 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 will return a notification to the Sender advising the reason for that rejection.

(b) Future Dated Payments initiated on any particular Business Day after closure of the SWIFT PDS will be held in the SWIFT PDS queue pending dispatch and forwarded to RITS on the next Business Day.

(c) To assist in the assessment of liquidity requirements for the day, Framework 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. With commencement of the Daily Settlement Session the Payments will be placed on the System Queue and processed in the normal manner.

5.14 Recall Request

Where a SWIFT PDS payment is held on the System Queue or is a Warehoused Payment the Sender may seek return of the payment by issuing a recall request in accordance with the RITS Regulations.

5.15 Out of Hours Payment

(a) Payments sent "for value today" but dispatched to RITS after normal RITS operating hours, on any particular Business Day, will be ACKed by the SWIFT Messaging Service and held in the SWIFT PDS 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 RITS will advise details of the rejection to the Sender.

(b) Payments sent "for value today" but dispatched to RITS, on any particular Business Day, before RITS operating hours will be ACKed by the SWIFTNet Copy Service and held in the SWIFT PDS Queue pending opening of RITS on that Business Day.

5.16 Sender Notification

On advice from RITS of settlement, SWIFT will send settlement details to the Sender advising full details of the settlement, including the Sender's RITS Allocation balance following settlement of the Payment.

5.17 Rejection of Payment

(a) When RITS is unable to process a payment, SWIFT will send details of rejection of that payment to the Sender advising the reason for the rejection.

(b) On closure of the Settlement Close Session, RITS will automatically reject each payment remaining on the System Queue and SWIFT will send details of that rejection to the Sender advising the reason for the rejection.

5.18 Receiver Payment Order

On advice from RITS of Settlement, SWIFT will identify the original payment message, add the settlement information in the SWIFTNet Header of the payment message, and forward the original Payment with the additional settlement particulars to the Receiver.

5.19 Undelivered Message Reports

Full details regarding the above reports are available from the "SWIFT User Handbook".

5.20 Delivery Notifications

Framework Participants can choose to receive notice of delivery or a non-delivery warning, as applicable. Normal SWIFT fees will apply for the provision of these messages.

5.21 SWIFT CUG Fees

The SWIFT fee for payments processed across the SWIFT PDS CUG will vary from time to time as advised by SWIFT.

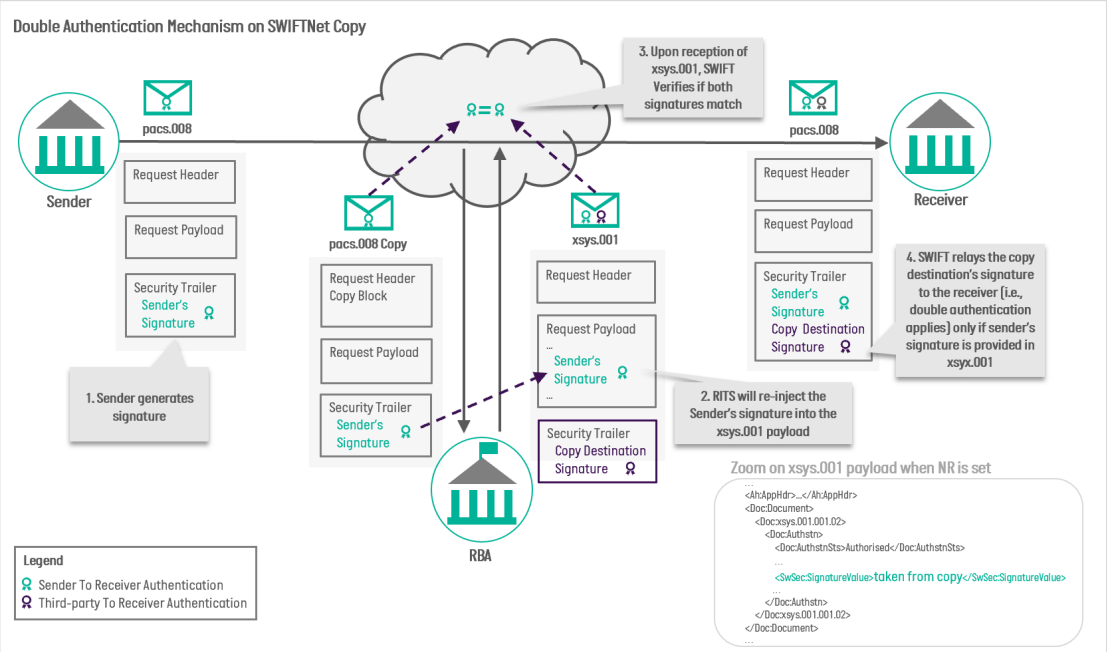
5.22 SWIFT Customer Support Centre

Normal SWIFT customer support centre facilities will be available should Framework Participants experience difficulties with the SWIFT system.

5.23 SWIFTNet Processes

(a) Double Authentication of Payment Messages

(i) The double authentication feature provides non-repudiation for the message recipient, i.e., assurance of the identity of the sender and that contents are unaltered, and assurance that settlement information has come from RITS unaltered. Double authentication will be automatically conducted on all payment messages (pacs.008, pacs.009 (CORE/COV) and pacs.004) transacted over Y-Copy in the ISO 20022 CUG. The double-authentication provides the Receiver with the Sender's signature from the original message together with the RITS signature of the authorisation response message, as shown below:



(b) Double authentication of payments provides the following security features:

(i) The Receiver can verify that the Sender's original signature is present together with the RITS authorisation signature (i.e. that settlement data relates to the original transaction).

(ii) SWIFT will verify that the Sender's signature is present on the incoming payment message, and that it matches the copy of the signature on the RITS xsys.001 *Authorisation/Refusal Response* (i.e. that the correct message has been authorised or refused).

(iii) The Sender can verify RITS signature covering the *Third Party To Sender Information* included in the xsys.002/003 *Authorisation/Refusal Notification* (i.e. that settlement data has not been altered).

(c) The only exception to double authentication of messages is during a contingency scenario pursuant to PART 9 when the copy mechanism is in T-Copy mode.

(d) The *Sender to Receiver* authentication and *Third-Party to Receiver* authentication elements are contained within the SWIFTNet Header. Framework Participants should review the SWIFTNet Header and when receiving payments, should ensure that both signatures are present. As SWIFT retains messages for 124 days, Framework Participants should consider their long-term archival requirements for these elements.

(e) Double authentication applies to payment messages which are processed through RITS. Framework Participants can optionally select the non-repudiation feature for those messages which are sent directly between Framework Participants (i.e. camt.029 and camt.056).

5.24 Retrieval of Messages from SWIFTNet

(a) Framework Participants can retrieve their sent and received InterAct store-and-forward messages and files from the SWIFTNet by:

(i) sending an xsys.015 (*Retrieval Request*) message; or

(ii) a request via the SWIFTNet web application.

(b) The retrieved messages will be delivered to a store-and-forward queue.

(c) Alternatively, Framework Participants can request a short-term bulk message retrieval which will be delivered via FileAct.

(d) Note that limits apply to retrieval periods based on the type of request made. More information about these processes can be found in the “SWIFTNet Messaging Operations Guide”.

5.25 Store-and-Forward Message Retransmission

In store-and-forward messaging mode, SWIFT stores a Sender’s message or file on a delivery queue in the central SWIFTNet systems. The message remains in the queue until the Receiver connects to SWIFTNet and is ready to receive it. More information about this process can be found in the “SWIFTNet Messaging Operations Guide”.

The next page is Part 6

PART 6 AUTOMATED INFORMATION FACILITY (AIF)

6.1 AIF Availability

(a) 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 Messaging Service utilising RITS AIF.

(b) 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 Framework Participant'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.

(c) A range of RITS AIF unsolicited messages and reports are also available to Framework Participants via the SWIFT Messaging Service.

6.2 Central Site AIF Destination Code

(a) The RITS central site SWIFT destination code for AIF messages (commands, enquires and unsolicited messages) is *RSBKAUSR*. Framework Participants utilising the service must ensure that AIF messages forwarded to RITS record the above mentioned destination code.

(b) Full details regarding RITS AIF are contained in the RITS Regulations and "RITS User Handbook".

6.3 MT and MX Migration Considerations[16]

(a) The AIF uses MT messages exchanged over SWIFTNet. All relevant RITS AIF messages (e.g. ESA statements) cater for both MT and MX payments sent to RITS for settlement. [17]

(b) From November 2024 RITS AIF will commence a period of coexistence where AIF messaging is available both in MT and ISO 20022 formats. For details on using the ISO 20022 versions of RITS AIF messages, please contact the RITS Help Desk via rits@rba.gov.au.[18]

(c) Use of AIF MT Messages Relating to MX Payments[19]

[16] Amended effective 23/9/24, version 4 r&p 001.24
[17] Amended effective 23/9/24, version 4 r&p 001.24
[18] Amended effective 23/9/24, version 4 r&p 001.24

[19] Amended effective 23/9/24, version 4 r&p 001.24

(i) The following table details how the RBA will populate AIF MT messages with relevant details from the associated MX message. Further information on existing arrangements is available at https://www.rba.gov.au/rits/info/ritsswiftinterfaceuserguide.htm.

AIF MT Tag	AIF MT Field Name	ISO 20022 HVCS Field Name	Affected AIF Messages
21	Related reference	pacs.008 / pacs.009 (CORE/COV): *Instruction Identification* <Instrid> pacs.004: *Return Identification* <RtrId>	**Unsolicited advices:** MT198 SMT006 – *Change ESA Status Advice* (via RITS user interface) MT198 SMT009 – *Change Credit Advice* (via RITS user interface) MT198 SMT028 – *Pre-Settlement Advice* (Credit Level) MT198 SMT029 – *Pre-Settlement Advice* (ESA Level) MT198 SMT036 – *Post-Settlement Advice – Debit (Intrabank or Interbank)* MT198 SMT037 – *Post-Settlement Advice – Credit (Intrabank or Interbank)* **Commands:** MT198 SMT001 – *Recall Request* MT198 SMT004 – *Change ESA Status Request* MT198 SMT007 – *Change Credit Status Request* MT198 SMT031 – *Change ESA and Credit Status Request* **Enquiries:** MT942

AIF MT Tag	AIF MT Field Name	ISO 20022 HVCS Field Name	Affected AIF Messages
	TRN (part of the statement line)	pacs.008 / pacs.009 (CORE/COV): *Instruction Identification* <InstrId> pacs.004: *Return Identification* <RtrId>	**Unsolicited advices (ESA Statements):** MT942 SMT001 – *RITS ESA Interim Advice* MT950 SMT222 – *ESA Statement End of Day Advice* MT950 SMT888 – *RITS ESA Interim Session Statement Advice* MT950 SMT999 – *RITS ESA Reports Session Statement Advice*
	Transaction type code (part of the statement line)	N/A – The following logic will be used: • Where the original message type is a pacs.008 'S103' will be populated. • Where the original message type is a pacs.009 CORE or pacs.009 COV 'S202' will be populated. • Where the original message type is a pacs.004 and it is returning a payment from a pacs.008 'S103' will be populated. • Where the original message type is a pacs.004 and it is returning a payment from a pacs.009 CORE or pacs.009 COV 'S202' will be populated.	**Unsolicited advices (ESA statements):** MT942 SMT001 – *RITS ESA Interim Advice* MT950 SMT222 – *ESA Statement End of Day Advice* MT950 SMT888 – *RITS ESA Interim Session Statement Advice* MT950 SMT999 – *RITS ESA Reports Session Statement Advice*

The next page is Part 7

PART 7 FRAMEWORK PARTICIPANT TECHNICAL REQUIREMENTS

7.1 Environmental Requirements

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.

7.2 Primary Computer Site Overview

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

(b) The SCI 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 a UPS.

(c) 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.

7.3 Primary Site Communication Requirements

(a) The primary site must have a primary and secondary HSM. The second HSM must be tested at least once every six months, including Active-Active configurations to ensure adequate redundancy by demonstrating that each single site configuration can continue to operate if the primary HSM is removed from operation and the second HSM takes over.

(b) SWIFTNet connectivity

(i) Each Framework Participant must have two differently routed communication lines, each to a separate SWIFT Point of Presence (POP), i.e. a primary line and a secondary line.

(ii) 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:

(A) Be sourced from a separate service provider for each facility; or

(B) If the same service provider is used, then connectivity must be through diverse connection points.

(c) 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.

7.4 Back-up Computer Requirements

(a) 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.

(b) 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 clause 7.6. The two Back-up Tiers are:

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

(ii) Tier 2 Back-up: up to but not including 2.00% of Total National Transaction Value.

(c) 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.

(d) 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.

(e) The Company will advise each Framework Participant of the Back-up Tier applicable to that member annually along with the publication of the yearly audit compliance reminder issued in Q4 of each calendar year, or upon notification of a successful HVCS membership application.

7.5 Back-up Tier Allocation

(a) The Company will allocate Back-up Tiers based on each Framework Participant's percentage of Total National Transaction Value. The data used will be for the calendar Q3 period. Where a new Framework Participant joins the HVCS during the 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.

(b) If any Framework Participant reasonably believes that it should be allocated a different Back-up Tier, then that member may in writing provide justification and a request that the Company consider applying a different Back-up Tier. The Company will notify the Participant of the outcome of its consideration and make any change as it deems appropriate.

(c) 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 7.5, of the Back-up Tier which will apply to it.

7.6 Back-up Computer Site Overview

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.

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

(a) Each Framework Participant allocated Back-up Tier 1 must maintain, as a minimum requirement, a Back-up Computer Site which is geographically remote from its Primary Computer Site.

(b) A tier 1 Back-up Framework Participant must be able to:

(i) begin sending and receiving payments within two (2) hours in the event of a systems failure within the Primary Computer Site; or

(ii) 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.

(c) The Framework Participant must ensure that its Back-up Computer Site is secure from unauthorised entry and that access to the area is controlled to protect against insider and external threats.

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

(e) The Back-up Computer Site, including SCI hardware and any related hardware essential to the continuous operation and availability of the system, must have a UPS.

(f) 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.

7.8 Tier 2 Back-up – Single Building Back-up Computer Site Requirements

(a) Each Framework Participant allocated Back-up Tier 2 must maintain, as a minimum requirement, a Back-up Computer Site. Each Back-up Tier 2 Framework Participant 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 Back-up Tier 1 Framework Participants.

(b) The Framework Participant must ensure that its Back-up Computer Site is secure from unauthorised entry and that access to the area is controlled to protect against insider and external threats.

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

(d) The Back-up Computer Site, including SCI hardware and any related hardware essential to the continuous operation and availability of the system, must have a UPS.

(e) 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.

(f) A tier 2 Back-up Framework Participant must be able to:

(i) begin sending and receiving payments within four (4) hours in the event of a systems failure within the Primary Computer Site; or

(ii) 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.

(g) Although a geographically remote Back-up Computer Site is not mandatory for Back-up Tier 2 Framework Participants, a back-up site which is geographically remote from the Primary Computer Site is strongly recommended.

7.9 Back-up Hardware and Software Requirements

(a) The adequacy of each Framework Participant's Back-up Computer Site arrangements and any supporting agreement required under this clause will be reviewed as part of the certification process.

(b) With the exception of Single Building Back-up Computer Sites, the Back-up Computer Site must contain at least one HSM.

7.10 Back-up Communication Requirements

(a) SWIFTNet connectivity

Subject to clause 7.7 (same building Back-up Computer Site) each Framework Participant must maintain at least one communication line 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.

7.11 Testing of Back-up Configuration

(a) 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. This requirement includes Active-Active configurations to ensure adequate redundancy by demonstrating that one site configuration can continue to operate if the other site is completely removed from operation. 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.

(b) Full details of all Back-up Computer Site system tests required to be carried out under this clause, 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.

7.12 System Availability

(a) Each Framework Participant must be logged on to the SWIFT PDS during the Core Business Hours.

(b) 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:

(i) Each tier 1 Back-up Framework Participant's system (which includes the SCI and the Core PPS) must meet a minimum of 99.7% up-time during the Core Business Hours on an annual basis.

(A) Following any disruption of processing during Core Business Hours, a tier 1 Back-up Framework Participant must substantially resume payments processing in accordance with this clause7.13.

(B) Failure to resume payments processing within the timeframes prescribed in this clause will result in formal reporting by the Member at the next Management Committee meeting.

(C) No single outage of any tier 1 Back-up Framework Participant's SCI and/or Core PPS may exceed four (4) hours duration and the aggregate duration of all such outages of a SCI 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.

(ii) Each tier 2 Back-up Framework Participant's system (which includes the SCI and the Core PPS) must meet a minimum of 99.5% up-time during the Core Business Hours on an annual basis.

(A) Following any disruption of processing during Core Business Hours, a tier 2 Back-up Framework Participant must substantially resume payments processing in accordance with this clause.

(B) Failure to resume payments processing within the timeframes prescribed in this clause as applicable will result in formal reporting by the Member at the next Management Committee meeting.

(C) No single outage of any tier 2 Back-up Framework Participant's SCI and/or Core PPS may exceed six (6) hours duration and the aggregate duration of all such outages of a SCI 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.

(c) The Provisions of this this clause apply equally to each Framework Participant's Primary Computer Site and Back-up Computer Site configurations.

(d) 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. The SWIFT PDS Log forms part of that Framework Participant's Yearly Audit Compliance Certificate.

(e) 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. Annexure D 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.

7.13 Minimum System Throughput Requirements

(a) Each Framework Participant's SCI must be capable of processing a minimum of 50% of its average daily SWIFT PDS transaction volume in any one hour (Average Hourly Transaction Volume 'AHTV'), including both inward and outward traffic and associated ACKs.

(b) 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.

(c) The provisions of this clause apply equally in respect of both the Primary Computer Site and Back-up Computer Site.

(d) Impaired Performance Monitoring and Reporting: Each framework Participant shall calculate the Required Hourly Transaction Volume (RHTV) as 400% of the Average Daily Transaction Volume (ADTV) used in the current years Yearly Audit Compliance Certificate, reduced to an hourly figure.

$$RHTV = \frac{ADTV * 4}{Core\ Business\ Hours}$$

During periods where the system throughput is degraded, records shall be maintained of the actual Transaction throughput achieved on an hourly basis. If the hourly throughput is below 51% of AHTV then a record shall be made of the event recording the percentage of RHTV, date, time, duration and when known, cause and remedial action.

Any such periods shall be reported in the Annual Compliance Audit Report in accordance with the following table:

Percentage of AHTV	Impaired Performance Period
50%	Report if period is 6 hours or greater
35%	Report if period is 5 hours or greater
25%	Report if period is 4 hours or greater
12%	Report if period is 3 hours or greater

7.14 Framework Participant Archival Requirements

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.

7.15 Initial Certification of Framework Participant's SWIFT PDS System

(a) Each Applicant must arrange for certification of its SWIFT PDS System by completing and submitting a System Certification Checklist. The System Certification Checklist must be in the form appearing in Annexure A and is to be completed and signed by a duly authorised officer of the Applicant.

(b) Copies of the System Certification Checklist and Certification Test Plan can be obtained from the Company by contacting the Secretary.

(c) Each Applicant must demonstrate, by completing the test scripts contained within the Certification Test Plan, that its SCI 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 test results, except as set out in in this clause, but a copy should be produced and retained for internal audit purposes. The Company may, as part of the verification process, request a Framework Participant to provide test results to assist in evaluation of the Certification results. In the event that a Framework Participant is unable to produce the requested 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.

(d) The completed System Certification Checklist and the test result forms required in terms of the Certification Test Plan are to be provided to the Secretary. 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 the Company can ensure that no misunderstanding of the test requirements has occurred.

(e) 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 must be promptly produced to the Secretary following the request.

(f) The Company will evaluate the test result forms, as set out in the Certification Test Plan, any test data provided in terms of this clause and the related System Certification Checklist, within fourteen (14) 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.

(g) 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.

(h) The Secretary will provide to the successful Applicant a System Compliance Certificate confirming and evidencing successful System Certification with respect to the SWIFT PDS.

(i) If the certification process fails in part, the Company will provide the applicant with details of the deficiency as part of its report, 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.

(j) Upon receipt of the additional certification documentation the Company will carry out a review of the material in terms of clause 7.16.

7.16 Yearly Audit Compliance

(a) Each Framework Participant must submit to the Company annually a Yearly Audit Compliance Certificate, in the form of Annexure B, 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.

(b) Framework Participants must report non-compliance with the SWIFT Customer Security Mandatory Controls in accordance with the Yearly Audit Compliance Certificate process (see Annexure C).

(c) 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 must be promptly produced to the Secretary following that request. See also Annexure B for further instructions on the procedural requirements in relation to Yearly Audit Compliance Certificates.

7.17 Failure to Meet Technical Requirements

(a) If the Yearly Audit Compliance Certificate given by a Framework Participant in accordance with clause 7.16 reveals that a Framework Participant has failed to meet any of the technical requirements specified in this Part 7, the Company will, subject to this clause7.18, notify the Framework Participant of the deficiency, in writing, requesting rectification of the deficiency within 30 days of the date of that notice.

(b) If any deficiency specified in any notice issued by the Company in accordance with this clause 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.

(c) If, in the opinion of the Chief Executive Officer, the deficiency notified in accordance with this clause 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.

7.18 SCI Modifications and Upgrades

(a) Any Framework Participant implementing any new SCI must successfully complete the normal initial certification process, in accordance with clause 7.16, prior to implementing the new configuration.

(b) Any Framework Participant implementing any upgrade or modification of its existing SCI, 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.

(c) If a Framework Participant upgrades or modifies, or proposes to upgrade or modify, its SCI, 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.

(d) The Management Committee may then review the particulars of that, or that proposed, upgrade or modification provided to it under this clause and may issue such instructions as it considers necessary to ensure that the upgraded or modified SCI 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 Part 8

PART 8 SWIFT PDS MESSAGE CONTENT SPECIFICATIONS

8.1 Message Types [20]

(a) This section outlines the payment message types that make up the ISO 20022 message set, which are shown in the table below. Systems messages are generated as part of the SWIFTNet Copy Service, so Framework Participants need only receive them. All xcop.001 and xsys.001 messages are transacted exclusively between SWIFT and RITS.[21]

Message Type	Definition
BAH (head.001)	
head.001	BAH
Payments clearing and settlement messages (pacs.xxx)	
pacs.008	FI to FI Customer Credit Transfer
pacs.009 CORE	FI Credit Transfer CORE
pacs.009 COV	FI Credit Transfer COV
pacs.004	Payment Return
Exception and investigation messages (camt.xxx)	
camt.056	FI to FI Payment Cancellation Request
camt.029	Resolution of Investigation
SWIFTNet Copy Service message set (xcop.001/xsys.xxx)	
xcop.001	Partial Copy Message
xsys.001	Y-Copy Authorisation or Refusal
xsys.002	Y-Copy Authorisation Notification
xsys.003	Y-Copy Refusal Notification
xsys.010	Non-Delivery Warning
xsys.011	Delivery Notification

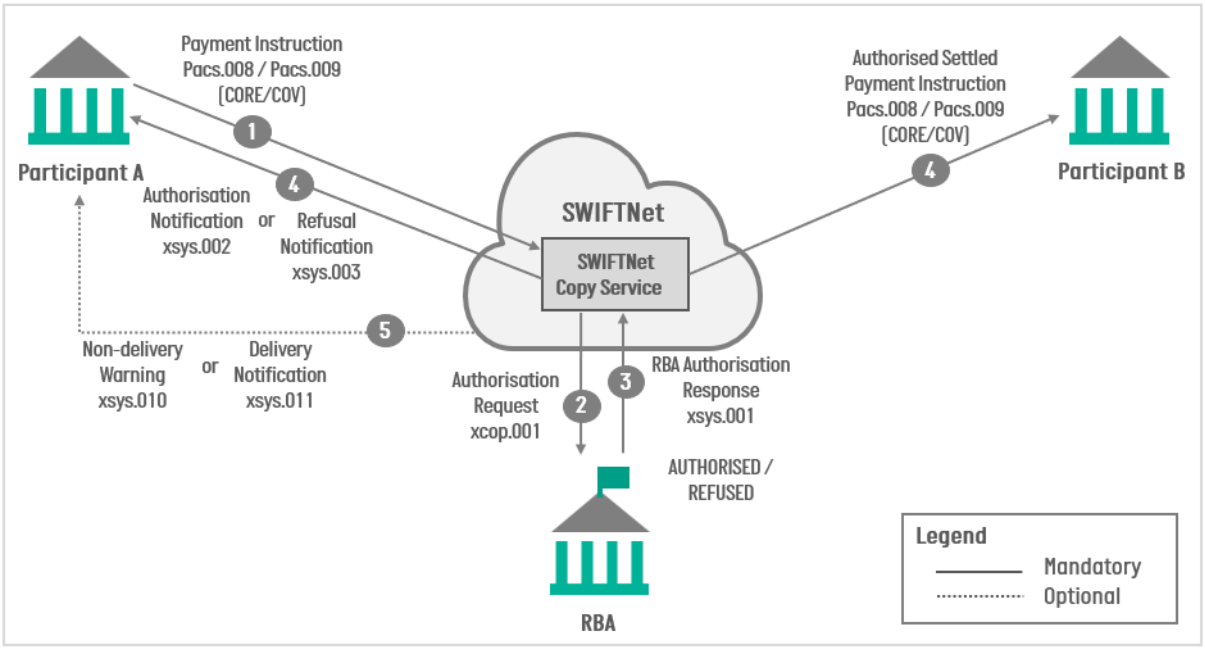
(b) Only system (xsys.xxx) messages that relate to payment settlement are in scope for the HVCS, although a number of additional system messages can be used by Framework Participants, notably, the xsys.015 *Retrieval Request*. Full details of these messages are also contained in the "SWIFTNet System Messages Guide".

(c) Further information on the base ISO 20022 standard is available at www.iso20022.org and information on the SWIFTNet Copy Service message set is available at www.swift.com.

8.2 Message Flow – Settlement

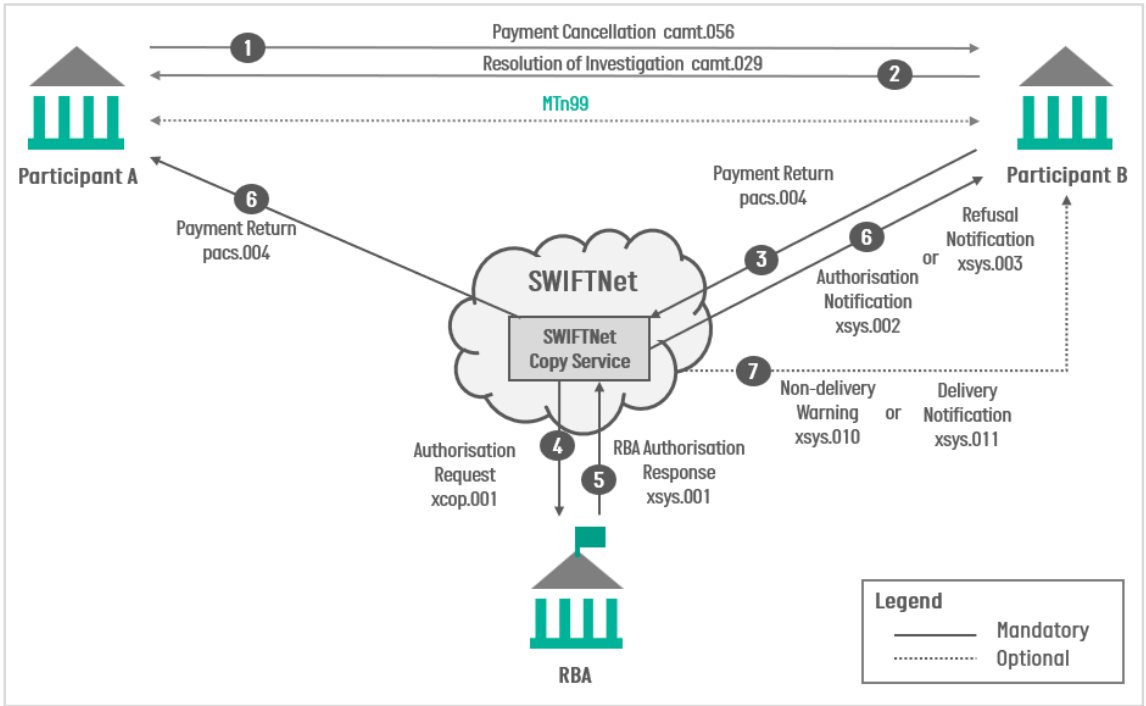
The table below sets out the MX settlement message flow.[22]

[20] Amended effective 23/9/24, version 4 r&p 001.24
[21] Amended effective 23/9/24, version 4 r&p 001.24
[22] Amended effective 23/9/24, version 4 r&p 001.24



8.3 Message Flow – Payment Return

The table below sets out the message flow on MX payment return.[23]



[23] Amended effective 23/9/24, version 4 r&p 001.24

8.4 Participation Obligations

(a) The MUGs contain the technical message format and usage guidelines for each ISO 20022 message definition, while this Part 8 provides additional market practice guidance. Together these documents provide the overall framework for the operation of the ISO 20022 CUG and Framework Participants must adhere to all mandatory requirements contained in the MUGs and these Procedures.

8.5 MUGs

(a) MUGs have been derived from each base ISO 20022 message and adapted to meet Australian market practice needs by applying further restrictions while retaining consistency with the global standard– for example by:

(i) Making optional fields mandatory;

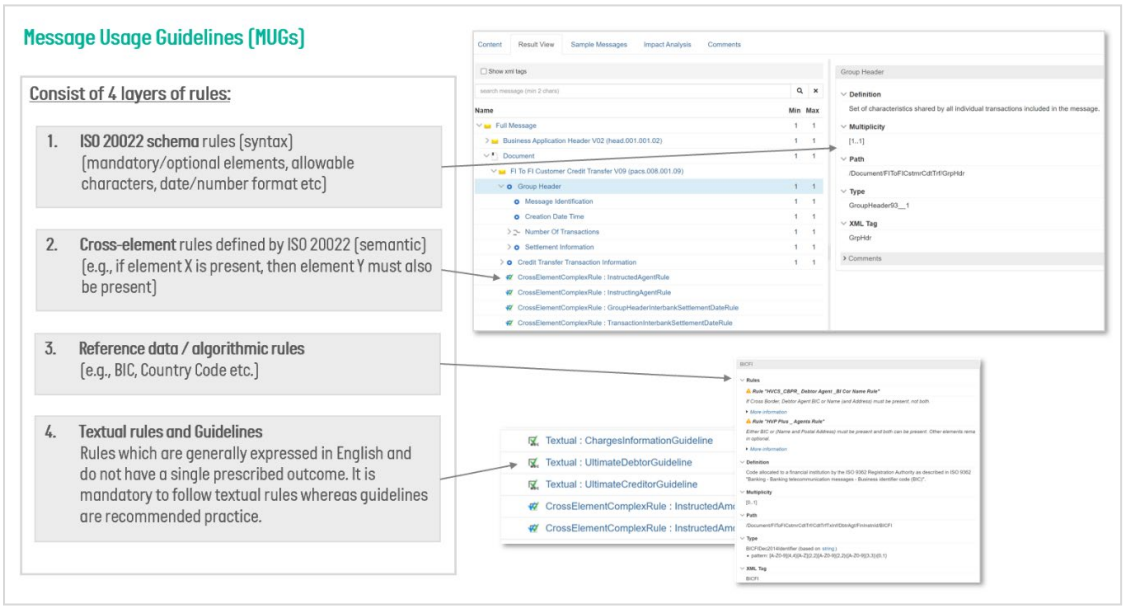
(ii) Disallowing a field;

(iii) Changing field parameters (e.g. reducing the maximum length, restricting the characters using a pattern); or

(iv) Changing the multiplicity of a field (e.g. make it non-repetitive).

(b) This is illustrated by the diagram below:

(c) The MUGs are comprised of different types of rules as described in the diagram below.



8.6 Message Validation

(a) For the purposes of validation, the rules in the MUGs fall into two categories:

(i) Formal rules or 'hard' rules – which include the schema, cross-element and reference data rules. These can be articulated in the form of a machine-readable algorithms and can be easily validated; and

(ii) Textual rules – which include textual rules and guidelines which are not able to be validated in a deterministic way.

8.7 SWIFTNet Validations

(a) Basic validation is performed centrally by SWIFT on all messages submitted on SWIFTNet to ensure the XML tree is well formed and that the message complies with the base ISO 20022 message format.

(b) The XML validations ensure that the request payload contains valid XML coding, for example:

(i) Each XML document must be a single-rooted hierarchical structure of elements.

(ii) All elements must be correctly paired.

(iii) The element opening tag and closing tag are the same name.

(iv) Element names must start with an alphabetic character; subsequent characters may be alphanumeric.

(c) Message definition reports and schemas documents are listed in the SWIFT Knowledge Centre. These documents describe the detailed specifications and associated error codes for the base ISO 20022 message validations. These documents focus on the schema and cross-element validations that are conducted on the elements located inside the InterAct payload.

(d) Additional validations are performed to complement those described above. These consist of reference data and technical header validations, and are described in the SWIFT publication "Network Validation Rules for ISO 20022 messages".

(e) The HVCS CUG has been configured to perform base level message validation. Request Subtype in the SWIFTNet Header is only used where higher levels of validation are in place. For HVCS, therefore, the element must be left blank or the message will fail network validation.

(f) Any messages that fail validation will not be delivered.

(g) No further checking of HVCS traffic is undertaken, although those messages that originate from overseas are validated against CBPR+ requirements in FINplus.

(h) The SWIFTNet validations do not cover the formal rules contained within the MUGs, nor do they cover any textual rules found in the base ISO 20022 message and corresponding MUG.

8.8 Framework Participant Validations

The additional market practice restrictions imposed in the MUGs are not validated on the SWIFTNet. Framework Participants must ensure compliance with the MUGs through their own testing and quality assurance processes. Persistent non-compliance with message specifications will be addressed in the same way as any other breach of these Procedures.

8.9 Maintenance Process[24]

(a) The maintenance process establishes a framework for the HVCS for upgrading the ISO 20022 usage guidelines used domestically.[25]

(b) Maintaining the HVCS MUGs helps to ensure continued harmonisation and ongoing interoperability with ISO 20022 standards used by CBPR+ and other Market Infrastructures. It also allows the industry to make changes to the HVCS MUGs to support local requirements. [26]

(i) Maintenance Principles [27]

(A) ISO can publish a new version of the ISO 20022 standard up to once each year.

(B) ISO has an established process to maintain the standard, with a supporting structure of local, regional and global expert groups through which proposals for changes to the standard can be submitted. This process is described in detail on the ISO website. The HVCS version control framework intentionally does not duplicate or overlap with the ISO base version maintenance process. [28]

(C) HVCS will maintain its MUGs based on the principles and objectives of the HVPS+ ISO 20022 Payments Interoperability Charter. [29]

(D) The HVCS collection will be maintained to align with one of the two most recent HVPS+ template collections, including base message updates. [30]

(E) Sometimes technical changes will accommodate backwards compatibility to the previous standard. However, this will not always be possible.

(F) The HVCS will only operate on one collection at a time, meaning all Framework Participants must go live with the new collection at the

[24] Amended effective 23/9/24, version 4 r&p 001.24
[25] Amended effective 23/9/24, version 4 r&p 001.24
[26] Amended effective 23/9/24, version 4 r&p 001.24
[27] Amended effective 23/9/24, version 4 r&p 001.24
[28] Amended effective 23/9/24, version 4 r&p 001.24
[29] Amended effective 23/9/24, version 4 r&p 001.24
[30] Amended effective 23/9/24, version 4 r&p 001.24

same time. Members who do not upgrade and successfully certify will be unable to send HVCS payments.[31]

(G) The Company will issue release notes outlining changes each time a collection (the set of message usage guidelines) is changed. [32]

(H) Changes to the "External Code Lists" are published and managed by SWIFT as the registration authority for ISO 20022. They can occur quarterly and are not included in the HVCS version governance process. Framework Participants must maintain awareness of code list changes and maintain alignment in their back office.

8.10 Naming Conventions [Deleted][33]

8.11 Version Governance

(a) New versions of the base message and HVPS+ template will be assessed by the CCB when they become available. The CCB will decide whether to accept, defer, or ignore changes to the base standard and template, and how the resultant changes to the MUGs will be managed, including specification, publication, testing and implementation. [34]

(i) While the ISO 20022 Industry Migration Program remains active, it will govern changes to the MUGs, via the CCB and the IMSC. When the Program ends and maintenance transfers to BAU, the CCB will become an MC4 sub-committee.[35]

(ii) The CCB will endorse or reject each change and determine when changes should be made, including in some cases holding changes over until the next release, considering need, impact and urgency. [36]

(b) Release Management

(i) The HVCS release timeline will be planned to align with SWIFT's standards release for CBPR+.

(ii) The Company will facilitate an industry discussion around what change management approach would be appropriate, and plan high level milestones for the implementation taking into account the size of the changes and whether comprehensive industry testing is required. At this time, Framework

[31] Amended effective 23/9/24, version 4 r&p 001.24
[32] Amended effective 23/9/24, version 4 r&p 001.24
[33] Deleted effective 23/9/24, version 4 r&p 001.24
[34] Amended effective 23/9/24, version 4 r&p 001.24
[35] Amended effective 23/9/24, version 4 r&p 001.24
[36] Amended effective 23/9/24, version 4 r&p 001.24

Participants must also plan their own project timelines to meet the milestones set by the Company. [37]

(c) Industry Testing

(i) The Company will coordinate industry testing and adoption where such industry support is deemed necessary or beneficial.

(ii) The Company will maintain a testing suite that will form part of the version control process.

(d) Using the SWIFT MyStandards Readiness Portal

(i) During each collection release, the SWIFT MyStandards Readiness Portal will be updated with schema changes.[38]

(ii) The SWIFT MyStandards Readiness Portal will validate HVCS test messages using the same validation rules that are implemented in the HVCS CUG.[39]

(e) Forward Dated Transactions

(i) The HVCS will operate only one production collection at a time, with all Framework Participants going live on a new collection together. [40]

(ii) Framework Participants are able to send a pacs.008, pacs.009 or pacs.004 message with a settlement date up to 5 Business Days in the future. In the lead up to a version change Participants must not warehouse payments across a version change date. RITS validates message versions and will therefore reject any warehoused payments that span a version change. A warehoused payment created using version "n" cannot be processed on its value date when the live version has changed to "n+1". [41]

(iii) Note also that if Participants warehouse a forward dated message in-house, and then send it after a version change for that message type, it will be rejected by SWIFT, as the message version has been superseded and is no longer valid.[42]

8.12 Intermediaries and Correspondent Banks

(a) This section provides guidance in relation to requirements specific to Framework Participants who act as an intermediary.

(b) Framework Participants who act as an intermediary for incoming cross-border payments received in ISO 20022 must pass on those messages in accordance with the HVCS MUGs and without truncation, if they are to be processed in the HVCS

[37] Amended effective 23/9/24, version 4 r&p 001.24
[38] Amended effective 23/9/24, version 4 r&p 001.24
[39] Amended effective 23/9/24, version 4 r&p 001.24
[40] Amended effective 23/9/24, version 4 r&p 001.24
[41] Amended effective 23/9/24, version 4 r&p 001.24
[42] Amended effective 23/9/24, version 4 r&p 001.24

(excepting the use of the HVCS Bilateral Clearing Form and related contingency processes in the event of a Participant Outage). [43]

(c) The last SWIFT bank in the payment chain must update the SWIFT Universal Confirmation tracker.

The next page is Part 9

[43] Amended effective 23/9/24, version 4 r&p 001.24

PART 9 CONTINGENCY PROCEDURES

9.1 Application of Part 9

The provisions of this PART 9 are designed to enable orderly operation of the SWIFT PDS during a Contingency.

Contingency means:

A Disabling Event occurring at the:

(ii) Framework Participant level;

(iii) central site (RITS and CSI) level;

(iv) SWIFTNet level; or

(v) any event or other event or circumstance specified by the Management Committee for the purposes of this PART 9.

9.2 Application of Annexure J (HVCS Contingency Instructions)

(a) Where a Disabling Event occurring at the Framework Participant level prevents the Framework Participant from sending payments in the normal way (Participant Outage); or where a Disabling Event occurring at the central site level (RITS or CSI) prevents RITS from effecting settlement of payments in the normal way (RITS Outage), then the Contingency Instructions may also apply.

(b) During any period in which any provisions of this PART 9 apply, to the extent of any inconsistency, the Contingency Instructions will prevail over these provisions in PART 9 and over any other provisions of these Procedures.

9.3 Responsibilities

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

(b) 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.

9.4 Nature of Contingency

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

(i) A Disabling Event occurring at the Framework Participant level. Note that if the Disabling Event is a Participant Outage, the Contingency Instructions may also apply.

(ii) A Disabling Event occurring at the central site (RITS or CSI) level. Note if the Disabling Event is a RITS Outage, the Contingency Instructions may also apply.

(iii) A Disabling Event occurring at the SWIFT communication service (SWIFT Messaging Service) level. Note the Contingency Instructions do not apply to this type of Contingency.

(iv) Any other event or circumstance specified by the Management Committee and designated a Contingency for the purpose of this PART 9.

9.5 Framework Participant System Failure Overview

(a) The appropriate response to a Disabling Event 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 PART 7, 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.

(b) The Procedures set out in this PART 9 (and where applicable the Contingency Instructions) are designed to provide a framework within which each Framework Participant can consider its response to a particular Disabling Event, but it is recognised that outside factors, for example nature of the Disabling Event and the time of day that the problem occurs, might affect that Framework Participant's course of action, and where applicable, ability to comply with any contingency procedures in this PART 9 such as fallback to the Back-up Computer Site. In accordance with clause 9.6, a Framework Participant must immediately notify the System Administrator of any Disabling Event and in doing so must indicate:

(i) If the circumstances are such that the Framework Participant 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.

(ii) If the Disabling Event has or may cause a Participant Outage, the Framework Participant must:

(A) immediately notify the System Administrator in accordance with clause 9.7 and refer to the Contingency Instructions;

(B) immediately consider and discuss with the System Administrator that the Framework Participant's potential response may be to request the declaration of the Participant Fallback Period, during which the Framework Participant is permitted to send payments using the Participant Fallback Solution provided for in the Contingency Instructions; and

(C) use the Participant Outage runsheet in the Contingency Instructions as a guide for the time of day that any such decision to request or declare a Participant Fallback Period should be taken.

(c) Each Framework Participant experiencing a Disabling Event affecting its ability to receive inward Payments 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 inward

payments processing problems as soon as possible, either by correcting the problem with its Primary Computer Site or initiating fallback to its Back-up Computer Site.

(d) In all cases, a Framework Participant experiencing a Disabling Event must continue to manage its ESA liquidity position in RITS throughout the Disabling Event.

(e) Details of all SCI 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.

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

9.6 All Disabling Events to be Advised to System Administrator

(a) Any Framework Participant experiencing a Disabling Event which adversely affects its ability to send or receive payments in a normal way must immediately advise the System Administrator in accordance with clause 4.4. That Framework Participant must provide to the System Administrator brief details of the problem being experienced and, if applicable, give some indication as to when its SWIFT PDS System is likely to be operating as normal. This will assist the System Administrator in deciding whether or not to advise all Framework Participants of the issue.

(b) In accordance with clause 9.5, if the Framework Participant's Disabling Event has or may cause a Participant Outage, the Affected Participant must notify the System Administrator and discuss the potential for a Participant Fallback Period to be declared.

9.7 Advice of HVCS Framework Participants Experiencing a Disabling Event

If the System Administrator considers that a Framework Participant's Disabling Event is 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.

9.8 Advice of a Participant Fallback Period

If the Disabling Event has caused a Participant Outage, and a Participant Fallback Period has or could be declared, the System Administrator will advise all Framework Participants of this in accordance with the Contingency Instructions.

9.9 End-to-end Test of Fallback Solutions

Each Framework Participant must participate in an end-to-end test of Fallback Solutions provided for in the Contingency Instructions, occurring annually or as otherwise advised, on the dates specified by the Management Committee from time to time. Fallback testing applies equally to the MT and ISO 20022 CUGs, and consideration of equivalent requirements in volumes 1 and 2 of the HVCS Procedures should be taken into account together.

9.10 HVCS Processing Difficulties Contact Points

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 available on the Company's extranet.

9.11 HVCS Payments to Framework Participants Experiencing a Disabling Event

Framework Participants with payments to be sent to any Framework Participant experiencing a Disabling Event that affects its ability to receive inward payments 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 a Framework Participant experiencing a Disabling Event, as payments may be delayed in the SWIFT queue for some considerable time.

9.12 HVCS Payments to a Framework Participant During a Participant Fallback Period

(a) If a Framework Participant's Disabling Event causes a Participant Fallback Period to be declared, then Framework Participants with payments to be sent to the Affected Participant must continue to use SWIFT PDS, having regards to the liquidity implications and potential delays outlined above. The Participant Fallback Solution provides a means for the Affected Participant to send payments. It cannot be used as a means for the Affected Participant to receive payments outside of the SWIFT PDS.

(b) Framework Participants must, to the best of their ability, pause sending payments to an Affected Participant if requested to do so by the Affected Participant.

9.13 Simultaneous Failure of Framework Participant's Primary and Back-up Configurations

If a Framework Participant's Disabling Event causes both its Primary Computer Site and Back-up Computer Site to fail, such that it cannot fallback to the Back-up Computer Site and is prevented from sending or receiving payments in the usual way, then that Framework Participant will need to consider alternative arrangements for sending and receiving domestic high value payments.

9.14 Sending Payments

If the Disabling Event is preventing a Framework Participant from sending payments in the usual way (Participant Outage), the Contingency Instructions may apply and a Participant Fallback Period could be declared. During this time the alternative arrangements for the Affected Participant to send payments in the HVCS will be the Participant Fallback Solution provided for in the Contingency Instructions. In accordance with clause 9.5, the Affected Participant must notify the System Administrator of the Disabling Event and obtain approval to use the Participant Fallback Solution by means of a Participant Fallback Period being declared.

9.15 Receiving Payments

If the Disabling Event is preventing a Framework Participant from receiving payments in the usual way then that Framework Participant must be aware that in accordance with clause 9.12, their inbound payments will, subject to appropriate testing by RITS, continue to be settled and will be queued on that Framework Participant's SWIFT queue pending re-establishment of its connection. For the avoidance of doubt, and in accordance with clause 9.12, the Participant Fallback Solution cannot be used as a means for that Framework Participant to receive payments outside of the SWIFT PDS. Further, that Framework Participant must continue to manage its ESA position in RITS throughout the Disabling Event and may in some circumstances consider requesting that other Framework Participants limit or pause the dispatch of further payments until the Disabling Event is resolved.

9.16 Need for Framework Participants to Re-establish SCI Connection in the Shortest Possible Time

Payments forwarded to a Framework Participant experiencing a Disabling Event affective its inward payments processing will, subject to appropriate testing by RITS, be settled and queued on that Participant's SWIFT queue pending re-establishment of its connection. It is therefore imperative that the Framework Participant endeavour to re-establish its SCI connection either from the Primary Computer Site or Back-up Computer Site without delay.

9.17 Advise System Administrator When Disabling Event is Resolved

(a) Where any Framework Participant's Disabling Event is resolved, and if applicable, its SWIFT PDS System is operating again in the normal way, that Framework Participant must immediately advise:

(i) the System Administrator; and

(ii) if the System Administrator has issued a RITS broadcast message to all Framework Participants in respect of the problem, the Company of the change of status.

(b) If a Participant Fallback Period is in operation at the time that the Disabling Event is resolved, the Affected Participant must comply with the Contingency Instructions with respect to the continued use of the Participant Fallback Solution and reversion to the SWIFT PDS for sending payments.

9.18 RITS or CSI (Central Site) Disabling Event

(a) 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.

(b) 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 RTGS basis, because those payment delivery systems are unaffected by failure of the CSI.

9.19 Advice of RITS Central Site Failure

The System Administrator is responsible for advising all Framework Participants, of any Disabling Event occurring at the RITS or the CSI level, and any action initiated to correct the situation including the likely time until the system will be operating as normal. Advice by the System Administrator in accordance with this clause 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 on the Company extranet.

9.20 Resynchronisation of RITS Data Base

(a) The RBA 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 RBA will contact each Framework Participant to verify the ESA balance and associated transactions. Where a difference exists between the balance quoted by the RBA and a Framework Participant's position, the figure quoted by the RBA will be final.

(b) 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".

9.21 Central Communications Failure (SWIFT Messaging Service)

(a) Partial Communications Failure

(i) Standard SWIFT procedures set out in the "SWIFT User Handbook" will apply where the SWIFTNet or part of the SWIFTNet is experiencing difficulties.

(ii) 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 on the Company's extranet, and action proposed. If a notice in accordance with this clause is issued it will be necessary for Framework Participants to consider alternative arrangements for the dispatch of payments.

(b) Failure of Both RITS and/or CSI Primary & Back-up Configurations

(i) If a Disabling Event causes both RITS main site and back-up site to fail, or the main CSI and back-up to fail, the System Administrator will need to consider alternative means of processing payments. If the Disabling Event causes a RITS Outage the System Administrator:

(A) could recommend to the Company that a HVCS Fallback Period be declared during which time the HVCS Fallback Solution provided for in the Contingency Instructions will apply;

(B) must notify all Framework Participants if a HVCS Fallback Period has or could be declared; and

(C) will have regard to the timings in the RITS Outage runsheet timings in the Contingency Instructions and use this as a guide for the time of day that any such decision to declare a HVCS Fallback Period may need to be taken.

(ii) 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 on the Company's extranet.

(c) In the event that the System Administrator issues a RITS broadcast message under either clause 9.7, clause 9.19 or clause 9.21, or otherwise notifies HVCS Framework Participants of any other Contingency under PART 9 of these Procedures, then the Chief Executive Officer may, if they consider 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.

Note: clause 9.7 relates to a Framework Participant Disabling event, clause 9.19 relates to a central site (RITS or CSI) Disabling Event, and clause 9.21 relates to a SWIFTNet Disabling Event.

(d) Fallback Period

(i) 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 on the Company's extranet.

(ii) Any HVCS Fallback Period owing to a RITS Outage and Participant Fallback Period owing to a Participant Outage will be undertaken in accordance with the Contingency Instructions, unless otherwise agreed by the Company and advised by the System Administrator.

(iii) During a Fallback Period, every HVCS payment sent and received pursuant to the Fallback Solutions provided for in the Contingency Instructions is irrevocable at the time of receipt of that payment by the Receiver. For the avoidance of doubt, in relation to the Participant Fallback Solution, the reference to "receipt of that payment" in this clause means actual receipt by the Receiver of the hard copy or electronic form of the relevant payment instruction.

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

(e) Deferred Net Settlement

Subject to clause 9.25, where RITS cannot be used to effect settlement of HVCS payments on a RTGS basis, settlement must be conducted in accordance with clauses 9.21 to 9.24.

(f) Method of Settlement

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

(A) across ESAs using Fallback Settlement;

(B) for net of both the MT CUG and the ISO 20022 CUG; and[44]

(C) either for the multilateral net amount owing between each Framework Participant and all other Framework Participants or for the bilateral net amount owing between one Framework Participant and another Framework Participant.

(ii) Payments settled by RITS, prior to the decision to move to deferred net settlement in accordance with clause 9.21(d) are not affected by clauses 9.21(f) to 9.24 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.

(iii) For settlement under clause 9.21(e), 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 where applicable, for directly notifying the relevant settlement figures to the RBA. Where this is undertaken during a HVCS Fallback Period or a Participant Fallback Period, it must be done in accordance with the Contingency Instructions.

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.

[44] Amended effective 23/9/24, version 4 r&p 001.24

9.22 FTM Rules

(a) For settlement under clause 9.21(e), the FTM Rules are as follows:

(i) 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;

(ii) 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;

(iii) 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.

9.23 ESA Entries

The RBA will apply entries to the ESAs of Framework Participants in accordance with the final settlement figures calculated in accordance with this PART 9.

9.24 Interest Adjustment Where Settlement Delayed

(a) 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.

(b) The RBA will record the net balance owing to or by each Framework Participant for each day on which it dispatched 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.

(c) The RBA 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.

9.25 Failure to Settle

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.

9.26 Settlement Contact Points

The primary and fallback contact details and numbers to be used to contact the RBA and the settlement contact points for each Framework Participant are available on the Company's extranet. Each Framework Participant must notify the RBA 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 RBA of any change to its settlement contact point in accordance with this clause.

9.27 Errors and Adjustments to Totals of Exchanges

(a) All adjustments to totals caused by any error must be accounted for in the manner set out in this clause 9.28.

(b) 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 9.29) must be effected as follows:

(i) Errors of Magnitude

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

(1) where RITS is not, at the time of that agreement, functioning to effect settlements on a RTGS basis, the necessary adjustment must be made in the next Fallback Settlement, or

(2) where RITS is, at the time of that agreement, functioning to effect settlements on a RTGS basis, the necessary adjustment must be made by sending a Payment for same day value on that day, or

(B) 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:

(3) where RITS is not, at the time of that agreement, functioning to effect settlements on a RTGS basis, in the next Fallback Settlement after that day, or

(4) where RITS is, at the time of that agreement, functioning to effect settlements on a RTGS basis, by sending a Payment for same day value no later than on the next Business Day, and

(ii) Errors which are not Errors of Magnitude

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

(B) 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:

(5) where RITS is not, at the time at which the error is found, functioning to effect settlements on a RTGS basis the necessary

adjustment must be made in a Fallback Settlement on any of those days, or

(6) where RITS is, at the time at which the error is found, functioning to effect settlements on a RTGS basis the necessary adjustment must be made by sending a Payment for same day value on any of those days, or

(C) 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.

9.28 Interest Adjustments for Errors

(a) The interest payable pursuant to clause 9.27(b) will be calculated as follows:

(i) in respect of the first day - interest will be calculated at the ESR; and

(ii) 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.

9.29 Further Provisions Relating to Interest

If the Receiver and Sender concerned are unable to agree upon any question arising under clause 9.27, the provisions of Regulations Part 13 will apply.

9.30 Losses

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.

The next page is Part 10

PART 10 Cyber Fraud Event

10.1 Application of Appendix K1 (Cyber Fraud Instructions)

Where a Cyber Fraud Event occurs, then the Cyber Fraud Instructions will apply.

10.2 Fraud and Cyber Contact Point(s)

The Company will maintain a list of Cyber Fraud contact point(s) available on the Company's extranet.

The next page is Annexure A

ANNEXURE A SYSTEM CERTIFICATION CHECKLIST FOR MEMBERSHIP OF THE HVCS

(Clause 7.16)

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 Secretary.

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 cause of the 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 Secretary.

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 the Company as part of the Certification Test Factsheet. A copy 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 7.15 apply.

ANNEXURE A SYSTEM CERTIFICATION CHECKLIST FOR MEMBERSHIP OF THE HVCS

SYSTEM CERTIFICATION CHECKLIST[45]

TO: THE HVCS MANAGEMENT COMMITTEE SECRETARY
AUSTRALIAN PAYMENTS NETWORK LIMITED
SUITE 2, LEVEL 17,
GROSVENOR PLACE, 225 GEORGE STREET,
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

EMAIL ADDRESS

1. Environment - Primary Computer Site

a) A primary and secondary HSM are available (clause 7.3) (including Active-Active configurations) ☐

b) Two SWIFT communication lines, a primary and a secondary line for redundancy purposes, are available (clause 7.10). ☐

c) UPS is available and supplied to the SCI hardware configuration (clause 7.2). ☐

d) The area is fitted with adequate protection against fire, flood and water damage (clause 7.2). ☐

2. Environment - Backup Computer Site

a) **Tier 1 Back-up Applicants Only -** Backup computer site is geographically separate from the primary site (clause 7.7). ☐

[45] Amended effective 1/1/24, version 3 r&p 002.23

b) **Tier 2 Back-up Applicants Only -** Backup computer site configuration meets requirements (clause 7.8 and 7.9). ☐

c) **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 (clause 7.7). ☐

d) UPS is available and supplied to the SCI hardware configuration (clause 7.7). ☐

e) The area is fitted with adequate protection against fire, flood and water damage (clause 7.7). ☐

f) The Backup configuration is capable of moving to live operations within the approved timeframe (clause 7.7). ☐

3. Security

a) 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). ☐

b) All mandatory security control objectives as defined in the SWIFT Customer Security Controls Framework have been met.[46] (clause 5.1) ☐

4. System Availability (clause 7.12)

a) **Tier 1 Back-up Applicants only** - the system (which includes the SCI and the Core PPS) must be available at least 99.7% of the Core Business Hours. The level of system redundancy is designed to ensure: ☐

(i) No single outage will exceed four (4) hours. ☐

(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. ☐

b) **Tier 2 Back-up Applicants only** - the system (which includes the SCI and the Core PPS) must be available at least 99.5% of the Core Business Hours). The level of system redundancy is designed to ensure: ☐

(i) No single outage will exceed six (6) hours. ☐

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

(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. ☐

5. System Performance

a) Primary SCI is capable of processing 50% of daily transaction volume in 1 hour (clause 7.13). ☐

b) Backup SCI is capable of processing 50% of daily transaction volume in 1 hour (clause 7.13). ☐

c) Specify estimated daily transaction volume (clause 7.5). ☐

d) Periods of system throughput degradation will be logged and reported if they reach the levels specified in the table below (clause 7.13). ☐

Percentage of AHTV*	Impaired Performance Period
50%	Report if period is 6 hours or greater
35%	Report if period is 5 hours or greater
25%	Report if period is 4 hours or greater
12%	Report if period is 3 hours or greater

* AHTV is average daily SWIFT PDS transaction volume in any one hour, including both inward and outward traffic and associated Acknowledgements

6. Operations

a) SWIFT PDS messages are stored on a suitable medium for a minimum of 7 years (clause 7.14). ☐

b) 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. Certification Test Plan Results

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

(i) Certification Test Factsheet; ☐

(ii) Specific Conditions Test Checklist; and ☐

(iii) Community Test Checklist. ☐

b) Full details of test script results required in terms of clause 7.15 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.

ANNEXURE A SYSTEM CERTIFICATION CHECKLIST FOR MEMBERSHIP OF THE HVCS

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 Annexure B

ANNEXURE B YEARLY AUDIT COMPLIANCE CERTIFICATE FOR CONTINUING MEMBERSHIP OF THE HVCS

(Clause 7.16)

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 7.17 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 Secretary.

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 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.

Framework Participant is required to maintain a SWIFT PDS Log (see clause 4.8) containing details of:

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

(b) 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

(c) 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 Secretary.

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

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.

ANNEXURE B YEARLY AUDIT COMPLIANCE CERTIFICATION FOR CONTINUING MEMBERSHIP OF THE HVCS

YEARLY AUDIT COMPLIANCE CERTIFICATE[47]

TO: COMPLIANCE MANAGER
AUSTRALIAN PAYMENTSNETWORK LIMITED
SUITE 2, LEVEL 17,
GROSVENOR PLACE, 225 GEORGE STREET,
SYDNEY 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

EMAIL ADDRESS

1. Environment - Primary Computer Site

a) A primary and secondary HSM are available (clause 7.3) (including Active-Active configurations) ☐

b) The secondary HSM was tested once every six months (clause 7.4) ☐

c) Two SWIFT communication lines, a primary and a secondary line for redundancy purposes, are available (clause 7.10). ☐

d) UPS is available and supplied to the SCI hardware configuration (clause 7.2). ☐

e) The area is fitted with adequate protection against fire, flood and water damage (clause 7.2). ☐

f) The secondary SWIFT communication line was tested on a minimum of four times during the year (clause 7.3). ☐

[47] Amended effective 1/1/24, version 3 r&p 002.23

2. Environment - Backup Computer Site

a) **Tier 1 Back-up Framework Participants Only** - Backup computer site is geographically separate from the primary site (clause 7.7). ☐

b) **Tier 2 Back-up Framework Participants Only** - Backup computer site configuration meets requirements (clause 7.8 and 7.9). ☐

c) **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 (clause 7.11). ☐

d) UPS is available and supplied to the SCI hardware configuration (clause 7.7). ☐

e) The area is fitted with **adequate** protection against fire, flood and water damage (clause 7.7). ☐

f) **Tier 1 Back-up Framework Participant Only** - The backup configuration's ability to move to live operations, with the required timeframes, was successfully tested at least twice during **the** year (clause 7.11 and 7.7) (including Active-Active configurations). ☐

g) **Tier 2 Back-up Framework Participants Only** - The backup configuration's ability to move to live **operations**, with the required timeframe, was successfully tested at least twice during the year (clause 7.7 and 7.11). ☐

3. Security

a) **Operating** system security which runs on the SCI hardware functionally conforms to the SWIFT **Customer** Security Controls Framework (clause 5.1). ☐

4. System Availability (clause 7.12)

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

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

(ii) No single outage exceeded four (4) hours; 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. ☐

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

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

(ii) No single outage exceeded six (6) hours; 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. ☐

5. System Performance

a) Primary SCI is capable of processing 50% of the daily transaction volume in 1 hour (clause 7.13). ☐

b) Backup SCI is capable of processing 50% of the daily transaction volume in 1 hour (clause 7.13). ☐

c) Periods of system throughput degradation will be logged and reported if they reach the levels specified in the table below (clause 7.13)

Percentage of AHTV*	Impaired Performance Period
50%	Report if period is 6 hours or greater
35%	Report if period is 5 hours or greater
25%	Report if period is 4 hours or greater
12%	Report if period is 3 hours or greater

* AHTV is average daily SWIFT PDS transaction volume in any one hour, including both inward and outward traffic and associated Acknowledgements

6. Operations

a) SWIFT PDS messages are stored on a suitable medium for a minimum of 7 years (clause 7.14). ☐

7. SWIFT PDS Log

a) A SWIFT PDS Log has been maintained and all appropriate details recorded as required in terms of these Procedures (clause 4.8). ☐

8. SWIFT Customer Security Controls Framework

a) 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). ☐

b) All mandatory security control objectives as defined in the SWIFT Customer Security Controls Framework have been met (clause 5.1).[48] ☐

9. Fallback Mode Processes and Testing

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

b) The most recent end-to-end test of fallback mode as required under clause 9.9 of the Procedures was undertaken. ☐

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

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

relevant additional information) and to provide to the Company with that notification full particulars of that wrong or misleading information.

SIGNED FOR AND ON BEHALF

OF [NAME OF APPLICANT]:

_____

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 Annexure C

ANNEXURE C SWIFT CUSTOMER SECURITY MANDATORY CONTROLS NON-COMPLIANCE[49]

This form may be used by an HVCS Framework Participant to report non-compliance of the SWIFT Customer Security Mandatory Controls. Alternatively, Framework Participants may submit to the Company 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
SUITE 2, LEVEL 17,
GROSVENOR PLACE, 225 GEORGE STREET,
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 Annexure D

[49] Amended effective 1/1/24, version 3 r&p 002.23

ANNEXURE D INCIDENT REPORT[50]

This form may be used by an HVCS Framework Participant to report a breach of clause 7.12 as part of that Framework Participant's Yearly Audit Compliance Certificate or for the purposes of advising the Company of any such breach prior to completion of the Yearly Audit Compliance Certificate.

TO: RISK AND COMPLIANCE
AUSTRALIAN PAYMENTS NETWORK LIMITED
SUITE 2, LEVEL 17,
GROSVENOR PLACE, 225 GEORGE STREET,
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 _____

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

[50] Amended effective 1/1/24, version 3 r&p 002.23

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 Annexure E

ANNEXURE E GUIDELINES FOR CERTIFICATION WHEN USING TPPS

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 TPP to supply the infrastructure to meet the technical requirements set out in Annexure A System Certification Checklist and Annexure B Yearly Audit Compliance Certificate. This includes services commissioned as Infrastructure as a Service (IaaS) in the cloud.

Use of TPPs for provision of a complete service (provision of primary and backup site and application software) is only available to Tier 2 Framework Participants.

This document contains information on what requirements must be met by the TPP, 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.

		TPP	FP/A
1.	**Environment - Primary Computer Site**		
a)	A primary and secondary HSM are available (clause 7.3)	☑	☑
b)	The secondary HSM was tested once every six months (clause 7.4)	☑	
c)	Two SWIFT communication lines, a primary and a secondary line for redundancy purposes, are available (clause 7.10).	☑	☑
d)	UPS is available and supplied to the SCI hardware configuration (clause 7.2).	☑	☑
e)	The area is fitted with adequate protection against fire, flood and water damage (clause 7.2).	☑	☑
f)	The secondary SWIFT communication line was tested on a minimum of four times during the year (clause 7.3).	☑	☑
2.	**Environment - Backup Computer Site**		
a)	**Tier 2 Framework Participants** - Backup computer site configuration meets requirements (clause 7.8 and 7.9).	☑	☑
b)	UPS is available and supplied to the SCI hardware configuration (clause 7.7).	☑	☑
c)	The area is fitted with adequate protection against fire, flood and water damage (clause 7.7).	☑	☑
d)	**Tier 2 Framework Participants** - The Backup configuration's ability to move to live operations, with the approved timeframe, was successfully tested at least twice during the year (clause 7.7 and 7.11).	☑	

3. Security

a) Operating system security which runs on the SCI hardware functionally conforms to the SWIFT Customer Security Controls Framework (clause 5.1). ☑

4. System Availability (clause 7.12)

a) The system (which includes the SCI and the Core PPS) was available at least 99.5% of the core RITS hours during the last year. ☑

b) No single outage exceeded six (6) hours (clause 7.12). ☑ ☑

c) Yearly downtime did not exceed ten hours for those Framework Participants that do not participate in the Evening Settlement Session and thirteen hours for those Framework Participants that do participate in the Evening Settlement Session. ☑ ☑

5. System Performance

a) Primary SCI is capable of processing 50% of the daily transaction volume in 1 hour (clause 7.13). ☑

b) Backup SCI is capable of processing 50% of the daily transaction volume in 1 hour (clause7.13). ☑

c) Periods of system throughput degradation will be logged and reported if they reach the levels specified in the table below (clause 7.13) ☑

Percentage of AHTV*	Impaired Performance Period
50%	Report if period is 6 hours or greater
35%	Report if period is 5 hours or greater
25%	Report if period is 4 hours or greater
12%	Report if period is 3 hours or greater

* AHTV is average daily SWIFT PDS transaction volume in any one hour, including both inward and outward traffic and associated Acknowledgements

6. Operations

a) SWIFT PDS messages are stored on a suitable medium for a minimum of 7 years (clause 7.14). ☑

7. SWIFT PDS Log

a)	A SWIFT PDS Log has been maintained and all appropriate details recorded as required in terms of these Procedures (clause 4.8).	☑	☑

8. SWIFT Customer Security Controls Framework

a)	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).		☑
b)	All mandatory security control objectives as defined in the SWIFT Customer Security Controls Framework have been met.[51] (clause 5.1).	☑	☑

The next page is Annexure F

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

ANNEXURE F SUPPLEMENTARY MARKET PRACTICE

1. Business Application Header (head.001)

The BAH gathers together, in one place, data about the message, such as which organisation has sent the Business Message, which organisation should be receiving it, the identity of the message itself, and a reference for the message.

The purpose of the BAH is to provide a consistent and predictable way for this data to be conveyed with the message, regardless of implementation factors such as the choice of network. This does not prevent such data being conveyed either within the ISO 20022 message definition itself, or as part of a network header.

The BAH must accompany every pacs.xxx or camt.xxx message instance and, together, they make up the full message. For this reason, the BAH MUG is found in MyStandards at the start of each Business Message MUG.

The following sections provide market practice guidance for elements used in the BAH.

1.1 Guidance for Business Service and Financial Institution Identification

Element	Guidance
Business Service <BizSvc>	The Usage Identifier serves as a mechanism to identify the designated BAH *Business Service*, under which a message is exchanged, and when combined with the BAH *Message Definition Identifier* (e.g., pacs.009.001.09), to unambiguously identify a Business Usage on SWIFTNet/FINplus. The Usage Identifier: a. consists of a maximum of 35 characters with multiple sections (where each section has a maximum of 10 characters, separated with a full stop) containing only lowercase alpha-numeric characters; and b. comprises three sections, including: i. Short Issuer Organisation ID (mandatory [A]); ii. Business Context ID (one mandatory [B], additional IDs optional [C, D, …); and iii. Version (mandatory, fixed length of 2 characters [E]). The short issuer organisation ID will be 'apn' for all messages, and the first Business Context ID for all messages will be 'hvcs', with 'xbrdr' as the supplementary Business Context ID for all cross-border payments. The supplementary Business Context ID of 'xbrdr' must be used when: a. Framework Participants acting as intermediary create the domestic leg of a payment which has originated from cross-border for clearing through the HVCS; and b. Framework Participants send a payment through the HVCS to an intermediary Framework Participant for clearing to an overseas destination. Framework Participants who send or receive cross-border payments that have an HVCS domestic leg (including using non-SWIFT networks) must also ensure the supplementary Business Context of 'xbrdr' is used. Note: a. The Usage Identifier has a version number that reflects the profile of the SWIFTNet Copy Service. It evolves independently of the version number of the ISO message type on which the Usage Identifier has been defined and is considered in line with the overall version control process established for all HVCS messages. b. In the HVCS, for example; the Usage Identifier can be used to distinguish multiple different business contexts (services) as required (e.g., apn.hvcs.xbrdr.01).

	Agreed Usage Identifiers are noted below: **Business Service Usage Identifier** / **Recommended Usage** apn.hvcs.01 — For domestic payment messaging across the HVCS apn.hvcs.xbrdr.01 — For an inbound/outbound cross-border transaction that is settling across the HVCS apn.hvcs.cov.01 — For a domestic pacs.009 COVER message across the HVCS (Note: when using a pacs.004 to return a domestic pacs.009 COV, use apn.hvcs.01) apn.hvcs.xbrdr.cov.01 — For an inbound/outbound cross-border pacs.009 COVER message that is settling across the HVCS (Note: when using a pacs.004 to return a cross-border pacs.009 COV, use apn.hvcs.xbrdr.01) apn.hvcs.inv.01 — For all Exception & Investigation messages (camt.029 and camt.056) Validation is performed in RITS to ensure a valid Usage Identifier is used in the HVCS. Please refer to Section 2.5.7 *Third Party Refusal Reason Codes (xsys.001 and xsys.003)* for more information. These Usage Identifiers are used when a message is sent through the HVCS between two Framework Participants domestically. When populating a message to be sent offshore, the *swift.cbprplus* Usage Identifier must be used. This is illustrated in the message flows presented in Section 2 *Payments Clearing and Settlement Messages.*
Financial Institution Identification *<FinInstnId>*	The 8-digit BIC must be published on the "SWIFTNet Directory" in order to pass SWIFT validation. The BIC8 in *Sender/Receiver DN* used in the SWIFTNet Header must be the same as the first 8 characters of the BIC11 contained in the *From/To* elements of the BAH. Similarly, the BIC11 used in the *From/To* elements of the BAH must be the same as the *Instructing Agent/Instructed Agent* BIC11 used in the message payload.

1.2 Guidance for Copy Duplicate and Possible Duplicate

Element	Guidance
Copy Duplicate <CpyDplct>	The *Copy Duplicate* <CpyDplct> indicator is a code to indicate whether the message is a copy, a duplicate, or a copy of a duplicate of a previously sent message. a. **COPY** indicates that the message is being sent as a copy to a party other than the account owner, for information purposes. b. **DUPL** indicates that the message is being sent as a duplicate of a message previously sent, for information/confirmation purposes. c. **CODU** indicates that the message is being sent as a copy to a party other than the account owner, for information purposes and the message is a duplicate of a message previously sent. Framework Participants can use the *Copy Duplicate* indicator in messages where a Y-Copy is not involved, for example, camt.029 and cam.056 messages and, if required, payment messages when

	the ISO 20022 CUG is in T-Copy (or fallback) mode. Framework Participants should consider adjusting their settlement calculations in this scenario. Duplicate checking is performed in RITS based on the combination of the *Instruction Identification* indicator (or *Return Identification* indicator for a pacs.004) and Sender BIC. RITS will only settle a transaction if the combination of Sender BIC and *Instruction Identification*/*Return Identification* is unique within the past 15 calendar days. RITS will ignore the *Copy Duplicate* indicator and will result in rejection of the copy or duplicate message due to the RITS duplicate checking processes. For this reason, it is not possible to use the *Copy Duplicate* indicator for payment messages which are settled through the RITS Y-Copy Service. The only time the *To* BIC in the BAH does not match the *Instructed Agent* BIC in the message body is when the *Copy Duplicate* indicator is set to COPY or CODU. When receiving a message with the *Copy Duplicate* indicator, Framework Participants must investigate whether the message is a duplicate to ensure it is not processed twice. The receiver should not assume duplicate messages will always arrive after the original message. If both instances of the message are received, one instance should be ignored. Framework Participants should have robust duplicate checking mechanisms in place and not rely solely on this element to identify duplicates.
Possible Duplicate <PssblDplct>	The *Possible Duplicate* <PssblDplct> indicator is used when: a. the sender has not received any reply and reasonable doubt exists about the delivery state of the original message; or b. the sender believes they have sent a message but is unable to find confirmation of it. The same Business Message is present, indicating it is possibly a duplicate of the first message. Although it is unlikely that a payment is sent into the Y-Copy and no *Authorisation Notification* or *Refusal Notification* is received, the *Possible Duplicate* indicator can be used to resend a payment. Duplicate checking is performed in RITS based on the combination of the *Instruction Identification* indicator (or *Return Identification* indicator for a pacs.004) and Sender BIC. RITS will only settle a transaction if the combination of Sender BIC and *Instruction Identification*/*Return Identification* is unique within the past 15 calendar days. RITS will ignore the *Possible Duplicate* indicator and may result in rejection of a possible duplicate message due to the RITS duplicate checking processes. When receiving a message with the *Possible Duplicate* indicator, Framework Participants should consider whether the message has been sent through the Y-Copy or not. Messages sent through the Y-Copy have passed RITS duplicate checking and are confirmed to be unique. These messages can be processed as required. However, when a non-Y-Copy message is received with the *Possible Duplicate* indicator, recipients must put in a process to investigate whether a is a duplicate to ensure it is not processed twice. The receiver should not assume duplicate messages will always arrive after the original message. If both instances of the message are received, one instance should be ignored. Framework Participants should have robust duplicate checking mechanisms in place and not rely solely on this indicator to identify duplicates. Note – the *Possible Duplicate* indicator is different to the *Copy Duplicate* indicator and the 'PDIndication' in the SWIFTNet Header.

The following table summarises the treatment of duplicated messages:

BAH Indicator	Y-Copy message (duplicate checking is performed in RITS)	camt.056 /29 message or pacs.xxx T-copy messages (no duplicate checking performed in RITS)
Copy Duplicate = COPY	Message will not be delivered (As the message will be refused by RITS, the COPY indicator should not be used in Y-Copy messaging)	Recipient must undertake duplicate checking before processing
Possible Duplicate = true	Recipient can process without duplicate checking as RITS will ensure uniqueness	Recipient must undertake duplicate checking before processing
Copy Duplicate = DUPL or CODU	Message will not be delivered (As the message will be refused by RITS, the DUPL or CODU indicator should not be used in Y-Copy messaging)	Message is for information only

In summary:

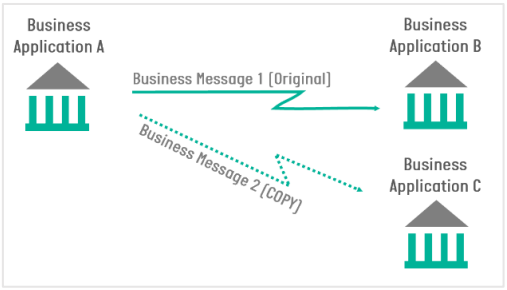
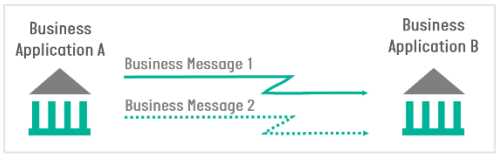
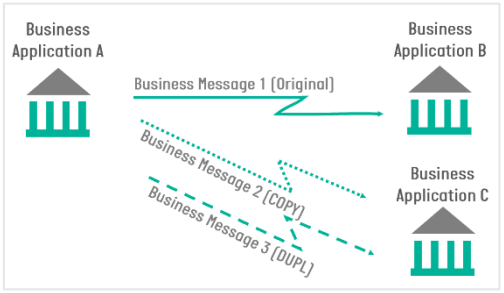
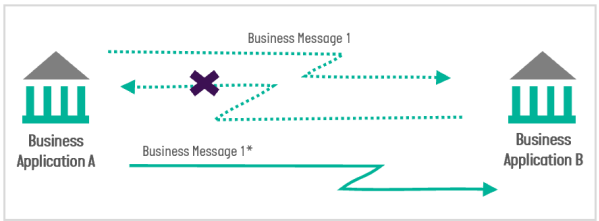
(a) The *Copy Duplicate* indicator must only be used on messages that are passed directly between Framework Participants (i.e. camt.xxx messages and payment messages when the SWIFT PDS CUG is in T-Copy mode);

(b) If used, the *Copy Duplicate* indicator may only have a value of either “true” or “false”; and

(c) Recipients must be able to recognise *Copy Duplicate* and *Possible Duplicate* transactions that are not passed through the Y-Copy and undertake a verification process to check whether the original message was received and/or processed.

The table below provides guidance for the population of the main elements in each scenario:

Scenario	Description
COPY – ‘copy’ Scenario Business Application A sends a copy of a previously sent Business Message	In this scenario, the following message elements apply: • ***From*****:** ID of Business Application A • ***To*****:** ID of Business Application C • ***Creation Date*****:** Date (and time) of the creation of this Business Application Header • ***Copy Duplicate*** = COPY • ***Related*****:** A copy of the relevant message elements of the Business Application Header of the original Business Message send to Business Application B

	
DUPL – 'duplicate' Scenario Business Application A sends a duplicate of a previously sent Business Message. The message is for information/confirmation purposes. It is a duplicate of a message previously sent. 	In this scenario, the following message elements apply: • ***From***: ID of Business Application A • ***To***: ID of Business Application B • ***Creation Date***: Date (and time) of the creation of this Business Application Header • ***Copy Duplicate*** = DUPL • ***Related***: A copy of the relevant message elements of the Business Application Header of the original Business Message
CODU – 'copy/duplicate' Scenario Business Application A sends a duplicate of a previously sent copy of a Business Message. Message is being sent as a copy to a party other than the account owner, for information purposes, and the message is a duplicate of a message previously sent. 	In this scenario, the following message elements apply: • ***From***: ID of Business Application A • ***To***: ID of Business Application C • ***Creation Date***: Date (and time) of the creation of this Business Application Header • ***Copy Duplicate*** = CODU • ***Related***: A copy of the relevant Message Elements of the Business Application Header of the copy Business Message.
Possible Duplicate = true Business Application A is unsure whether the original Business Message has been received and sends the same Business Message again, indicating it is possibly a duplicate. 	In this scenario, the following message elements apply: • ***From***: ID of Business Application A • ***To***: ID of Business Application B • ***Creation Date***: Date (and time) of the creation of this Business Application Header • ***Possible Duplicate*** = true • ***Related***: A copy of the relevant Message Elements of the Business Application Header of the original Business Message.

Use case scenarios are included in Annexure I to illustrate the use of these indicators.

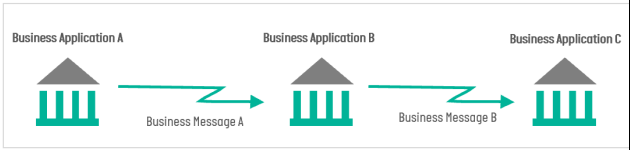
1.3 Guidance for *Related*

When a business process requires a previous Business Message to complete it, details of the previously sent/received message are captured in the *Related* element. As a Business Message may be related to other types of Business Messages, it is necessary to distinguish the function of the previous Business Message referred to (e.g. pacs.008 or pacs.009) in the *Message Definition Identifier*.

	Guidance
Related <Rltd>	The *Related* <Rltd> component enables the capture of the BAH from a related Business Message which has been previously sent or received. For example, when sending a camt.029 *Resolution of Investigation,* the underlying pacs.008 *FI To FI Customer Credit Transfer* should be referenced in the *Related* <Rltd> indicator. This would allow the receiver to apply specific processing to the message, based on the related information. The following elements are nested within the *Related* <Rltd> component, and where used, these contain the original data from the related BAH.

Element	Occurrences
From	Min 1 – Max 1
To	Min 1 – Max 1
Business Message Identifier	Min 1 – Max 1
Message Definition Identifier	Min 1 – Max 1
Business Service	Min 0 – Max 1
Creation Date	Min 1 – Max 1
Copy Duplicate	Min 0 – Max 1
Priority	Min 0 – Max 1

The table below provides guidance for the population of the main elements:

Scenario	Description
 This scenario is used when it is relevant for the recipient of Business Message B to know about the underlying Business Message A which triggered the creation of Business Message B.	In this scenario, the following message elements apply: • ***From*****:** ID of Business Application A • ***To*****:** ID of Business Application B • ***Creation Date*****:** Date (and time) of the creation of this Business Application Header (and Business Message) • ***Business Message Identifier*****:** The unique Identifier Business Message A

Scenario	Description
	• ***Message Definition Identifier***: Identification of the Message Definition e.g. camt.001.001.03 • ***Related*****:** A copy of the relevant Message Elements of the Business Application Header of Business Message A

The *Related* component is most commonly used as followings:

(a) To make reference to the original Business Message when using *Copy/Duplicate* or *Possible Duplicate* indicators;

(b) When populating a camt.056 or camt.029 with elements from the BAH of the pacs.008/pacs.009 or pacs.009 COV that is being requested to be returned; and

(c) When populating a pacs.004 with elements from the pacs.008/pacs.009 or pacs.009 COV that is being returned (e.g. if being returned via a different path).

Related is an optional indicator of the BAH as there are generally sufficient reference made to the related message within the payload. However, when using the *Copy Duplicate* indicator, the *Related* indicator must be populated.

2. Payments Clearing and Settlement Messages (pacs.xxx)

2.1 FI to FI Customer Credit Transfer (pacs.008)

The FI to FI Customer Credit Transfer message is the movement of an amount from a sending party account (the debtor account) to a beneficiary party (the creditor).

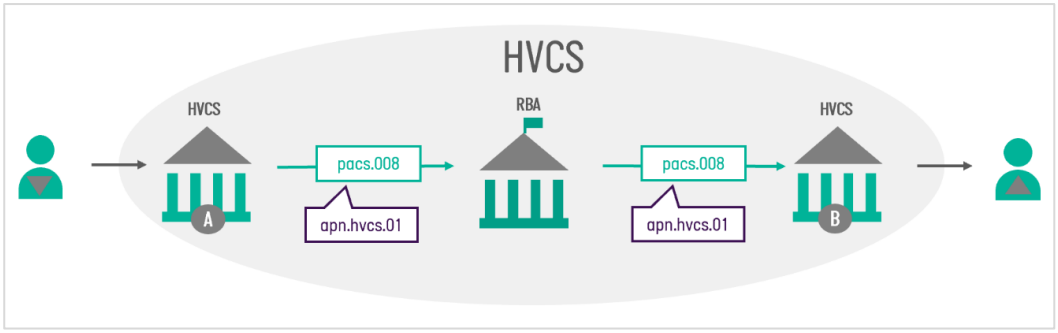
The pacs.008 (payments, clearing and settlement) message is the ISO 20022 MX Single Customer Credit Transfer.[52]

The scenarios below illustrate the movement of the pacs.008 message as it moves through the HVCS.

2.1.1 Scenario 1: The payment is being sent within the HVCS

The pacs.008 is sent from Framework Participant A to Framework Participant B via the HVCS.

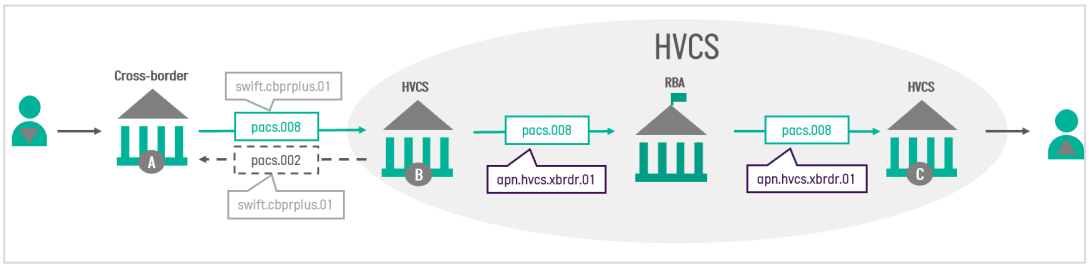
[52] Amended effective 23/9/24, version 4 r&p 001.24



2.1.2 Scenario 2: The payment is going to an end customer in the HVCS

(a) The pacs.008 is sent from FinPlus participant A to Framework Participant B via CBPR+;

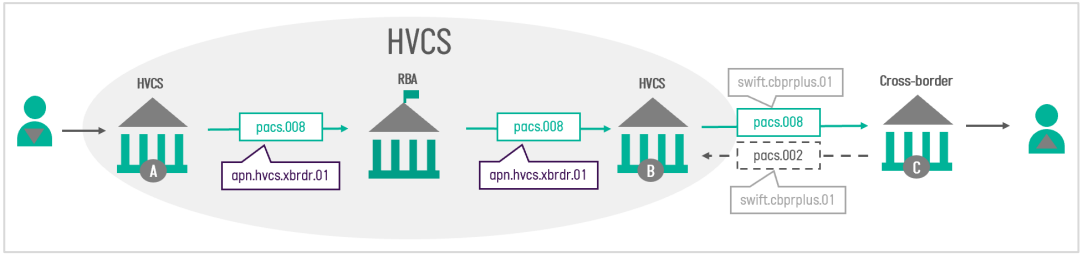
(b) Framework Participant B passes the message through the HVCS to Framework Participant C.



2.1.3 Scenario 3: The payment is sent from an HVCS Framework Participant to an offshore entity

(a) The pacs.008 is sent from Framework Participant A to Framework Participant B through the HVCS;

(b) Framework Participant B passes the message to CBPR+ participant C via FinPlus.



2.2 FI Credit Transfer (pacs.009 (CORE/COV))

The pacs.009 Financial Institution Credit Transfer message is sent by a debtor FI to a creditor FI, directly or through other agents and/or a payment clearing and settlement system. It is used to move funds from a debtor account to a creditor, where both debtor and creditor are FIs.

The pacs.009 has two main use cases:

(i) A CORE FI Credit Transfer message; and

(ii) A COV where it is used as cover for (to settle) a pacs.008.

(a) The pacs.009 COV, therefore, contains information about the underlying Customer Credit Transfer (pacs.008) for use in the cover scenario, which is the key difference between these two use cases.

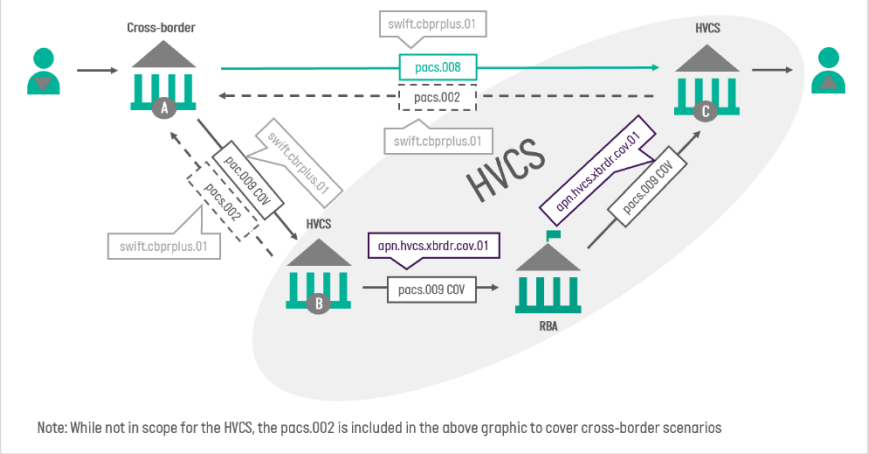
(b) The cross-border scenarios below illustrate the movement of the pacs.009 COV message as it moves in and out of the HVCS.

(i) Scenario 1: They payment is going to an end customer in the HVCS

(A) The pacs.008 is sent from FinPlus participant A to Framework Participant C via CBPR+;

(B) The pacs.009 COV goes from FinPlus participant A to Framework Participant B via CBPR+; and then from

(C) Framework Participant B to Framework Participant C via HVCS.

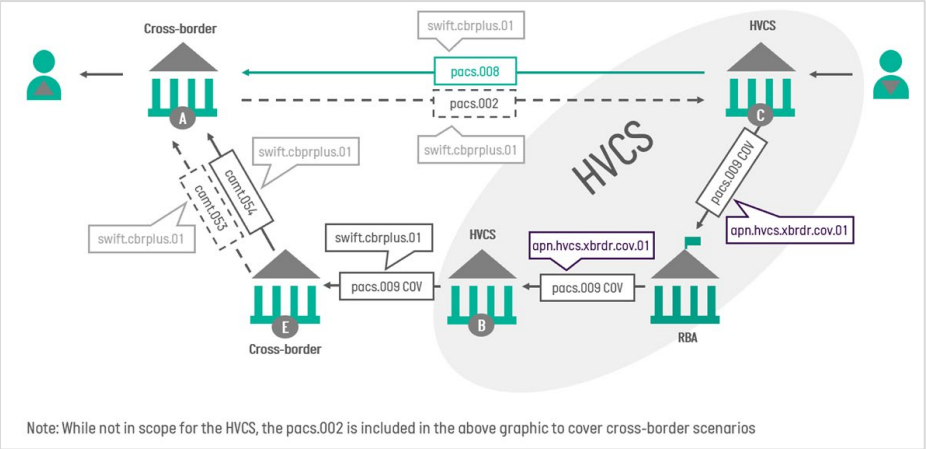


(ii) Scenario 2: The payment is sent from an HVCS Framework Participant to an offshore entity:

(A) The pacs.008 goes from Framework Participant C to Bank A via CBPR+;

(B) The pacs.09_COV goes from Framework Participant C to Framework Participant B via HVCS; and

(C) camt.xxx messages are sent from Framework Participant B to FinPlus participant A via CBPR+.



(iii) Scenario 3: The payment is going from an HVCS to a cross-border customer, the pacs.009 COV goes across multiple offshore entities

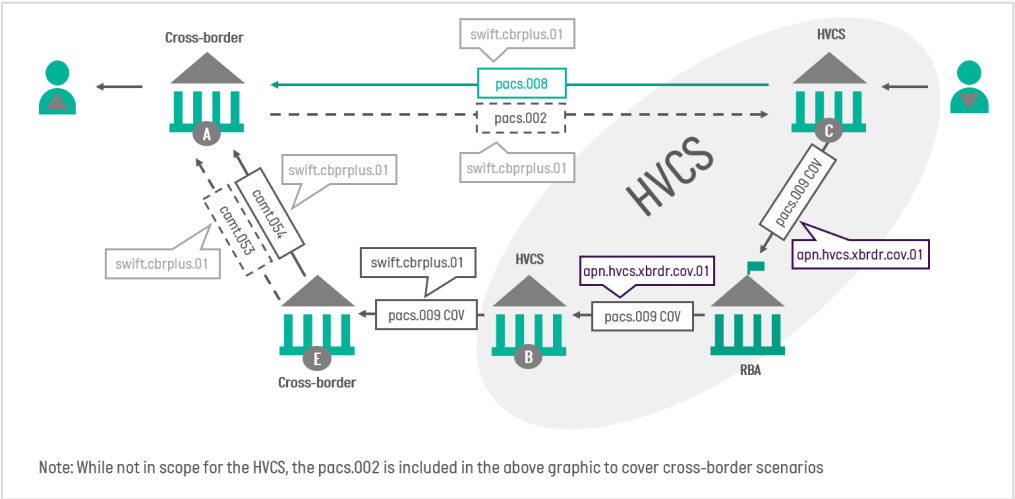
(A) The pacs.008 goes from Framework Participant C to FinPlus participant A via CBPR+;

(B) An additional offshore entity (FinPlus participant E) is added between Framework Participant B and FinPlus participant A:

(1) The pacs.009 COV goes from Framework Participant C to Framework Participant B via HVCS;

(2) Framework Participant B to FinPlus participant E via CBPR+; and then;

(3) A camt.xxx message would be sent from participant E to participant A



2.3 Payment Return (pacs.004)

(a) The pacs.004 Payment Return message is sent by an agent to the previous agent in the payment chain to return a payment which has previously settled.

(b) The Payment Return message refers to the original instruction(s) by means of references only, or by means of references and a set of elements from the original instruction. Payment returns may be the consequence of a payment cancellation requested by the Sender (solicited) or initiated by the Receiver as an unsolicited payment return.

(c) When using the pacs.004 message, it is important to note the following:

(i) Each pacs.004 message must only contain one payment return.

(ii) A Solicited Payment Return is a payment return requested by the payer FI through a Request for Payment Cancellation (camt.056).[53]

(iii) An Unsolicited Payment Return is a payment return initiated by the payee or payee FI.

(iv) The HVCS supports partial solicited payment returns with the use of multiple pacs.004 messages to return a payment in instalments. Participants must be able to receive multiple pacs.004 payment return instalments.

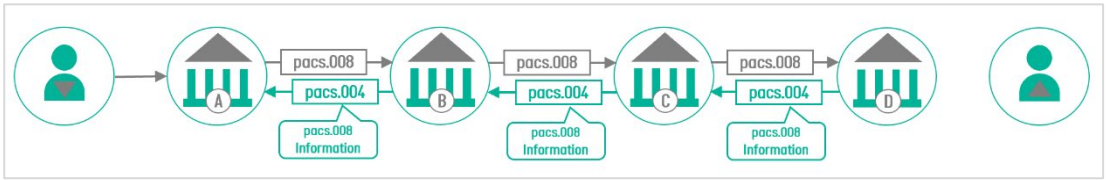
(v) In the HVCS, Unsolicited Payment Returns should be returned in one payment return.

(vi) Participants must be able to receive a Returned Interbank Settlement Amount that is different from the Original Interbank Settlement Amount due to currency exchange or charge fees.

(vii) The pacs.004 message must be used to return funds regardless of whether the return chain is the same as the original forward path or if it follows a different path.

(viii) Participants must not use the pacs.004 message to initiate a payment return of a payment return.

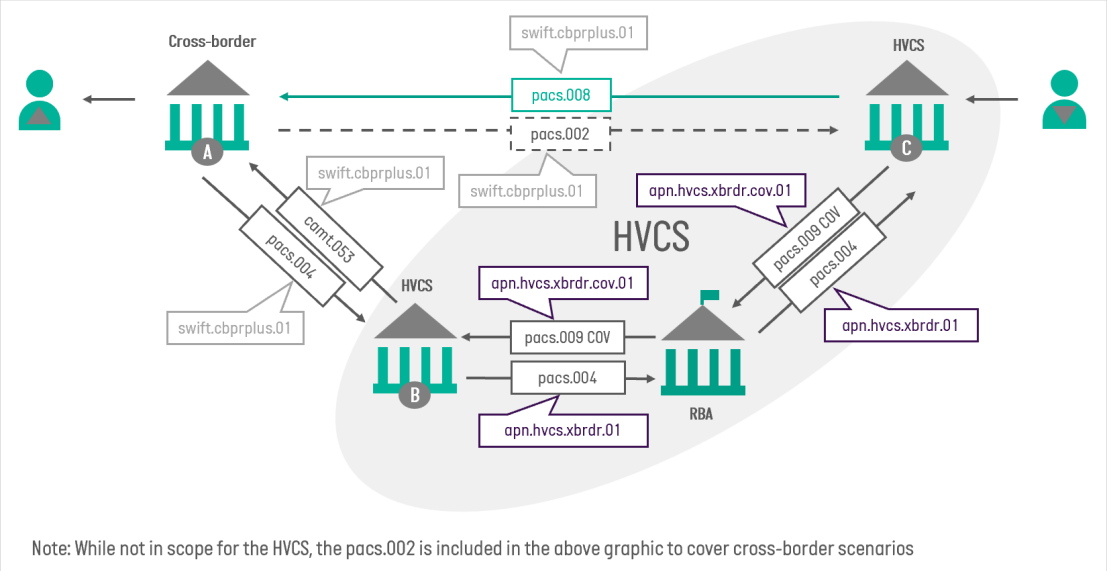
(ix) The pacs.004 is passed from one Framework Participant to another Framework Participant serially, as shown in the diagram below.



(d) The pacs.004 Payment Return uses a number of elements to capture details from the underlying payment it is returning, which are nested within the Original Group Information and Transaction Information. A number of these elements are mandatory within the HVCS to ensure pacs.004 conveys sufficient details to the receiving agent.

[53] Amended effective 23/9/24, version 4 r&p 001.24

(e) When returning a payment by the cover method, the pacs.004 follows the path of the pacs.009 COV message as shown below:



Note: While not in scope for the HVCS, the pacs.002 is included in the above graphic to cover cross-border scenarios

(f) Again, the pacs.004 message is sent serially between banks, this time referencing the pacs.009_ COV within *Original Group Information* and *Transaction Information*. The information of the underlying pacs.008 for which cover is provided must be captured in the underlying *Customer Credit Transfer* elements.

(g) When acting as intermediary, upon receipt of a pacs.004 instruction containing the elements (<OrgnlMsgNmId> = pacs.009 COV and <OrgnlTxRef> = pacs.008 details), the same path is to be taken regardless of whether the return originated domestically or cross-border.

(h) In some scenarios, for example if the intermediary Framework Participant was not involved in the original forward path, the intermediary may not have access to the original message details and must seek them in order to correctly populate the domestic pacs.004.

(i) More information about pacs.004 usage can be found in the Procedures clause 4.18**.**

2.4 Guidance for Elements (pacs.008 / pacs.009 (CORE/COV) / pacs.004)

This section provides market practice guidance for elements used in the pacs.008, pacs.009 (CORE/COV) and pacs.004 messages.

Element	Impacted Messages	Guidance
Creation Date <CreDt>	pacs.004 pacs.008	Time should be expressed as Local Time with Coordinated Universal Time (UTC) Offset in the format hh:mm:ss.sss+/-hh:mm. Inclusion of milliseconds is optional. For Australian time zones, the UTC Offsets are as follows:

<table>
<tr><td></td><td>pacs.009
(CORE/COV)

camt.029

camt.056</td><td>(a) Western Standard Time: +8 hours

(b) Central Standard Time: +9:30 hours

(c) Central Summer Time: +10:30 hours

(d) Eastern Time: +10 hours

(e) Eastern Summer Time: +11hours

By way of example, 10am in summer will be time stamped as follows:

(f) Perth - 10:00:00.000+08:00

(g) Brisbane - 10:00:00.000+10:00

(h) Sydney or Melbourne - 10:00:00.000+11:00</td></tr>
<tr><td>Message Identification

<MsgId>

Assignment Identification

<AssgnmtId></td><td>pacs.004

pacs.008

pacs.009
(CORE/COV)

camt.029

camt.056</td><td>The Message Identification element provides a point-to-point reference, as assigned by the instructing party, and sent to the next party in the chain to unambiguously identify all messages.

A fixed, 35-character format, following the below structure is to be used:

<table>
<tr><td>1-11</td><td>Sender's BIC [11] (BIC11 or BIC8 with 'XXX' suffix)</td></tr>
<tr><td>12 – 19</td><td>YYYYMMDD - Message Creation Date [8]</td></tr>
<tr><td>20 – 21</td><td>Channel/Processing System Identification [2]

Characters 20-21 can be used for internal channel / source identification, if the sending bank chooses so, otherwise the default value should be 00. Characters 20-21 can be populated with any alphanumerical value.</td></tr>
<tr><td>22 – 32</td><td>Number [11] which may be initialised at the start of each day (where ‘start of each day’ aligns with local time with UTC offset).

This number must be unique across all message types sent on the same day.</td></tr>
<tr><td>33 – 34</td><td>Fixed value 'HV' to indicate a HVCS payment [2]</td></tr>
<tr><td>35 – 35</td><td>Fixed value ‘0’ [1] (future use)</td></tr>
</table>

Note: The Message Creation Date used to populate characters 12-19 should align with the date populated in the Creation Date <CreDt> element which uses local time with UTC offset.</td></tr>
</table>

Instruction Priority <InstrPrty>	pacs.004 pacs.008 pacs.009 (CORE/COV)	HVCS Participants may consider entering into bilateral agreements and use this element for service differentiation.
Category Purpose <CtgyPurp>	pacs.008 pacs.009 (CORE/COV)	The Category Purpose element specifies the high-level purpose of the instruction based on a set of pre-defined categories. This is used by the initiating party to provide information concerning the processing of the payment. It is likely to trigger special processing by any of the agents involved in the payment chain. All valid Category Purpose codes can be used in the HVCS, or, where this element is populated in an inbound cross-border message, this element should be passed on as is. The full list of available codes be accessed here. Specific back office processes may apply when some codes are used. Expected processing and behaviour of additional codes will be defined as needed.
Instruction Identification <InstrId> *Return Identification* <RtrId>	pacs.008 pacs.009 (CORE/COV) pacs.004	The *Instruction Identification* <InstrId> indicator is a unique identification, as assigned by an instructing party for an instructed party, to unambiguously identify the instruction. It is a point-to-point reference that can be used between the instructing party and the instructed party to refer to the individual payment instruction. Usage:[54] (a) For ISO 20022 HVCS, usage is mandatory, restricted to maximum 16 characters. (b) It is used by RBA for settlement and duplicate checking (RITS transaction identification). The HVCS *Instruction Identification* element in the pacs.008 and pacs.009 messages must be structured as follows: (c) Usage is mandatory, maximum 16 characters (d) Characters 1-4: must not contain 'RITS', 'ACLR', 'ASXC', 'ASXB', 'MCIN' or 'ESSB (e) It must not start or end with a slash '/' or contain two consecutive slashes '//', and is limited to the following character set: 0-9 a-z A-Z / - ? : ( ) . , ' +, This same rule will also be applied to the HVCS *Return Identification* element in the pacs.004 message. The RBA completes duplicate checking by validating the combined values from the *Instruction Identification* and the Sender's BIC elements. It must not be the same *Instruction Identification* used within 15 calendar days since first being used. This means that if an *Instruction Identification* / *Return*

[54] Amended 23/9/24, version 4 r&p 001.24

		Identification was used on the 1st, it cannot be reused until the 16th. RBA does not check whether the *Copy Duplicate* <CpyDplct> and *Possible Duplicate* <PssblDplct> element is flagged. For interoperability with NPP, it is important to note where the unique RITS transaction Identification is populated: (f) For NPP, the RITS transaction identification is populated in the *Transaction Identification* element. (g) For HVCS, the RITS transaction identification is populated in the *Instruction Identification* element. (h) In both systems, the RITS transaction identification of a pacs.004 is populated in the *Return Identification* element.
End to End Identification <EndToEndId>	pacs.008 pacs.009 (CORE/COV)	The *End to End Identification* indicator is a value assigned by the initiating party. It must be carried through the entire payment chain and must not be overwritten. If the Initiation Party does not provide an *End to End Identification*, the element must be populated with "NOTPROVIDED". Recommended practice is to align with NPP's e-invoice payment ID rule, which was developed based on guidance from the ATO: For payment transactions assigned a category purpose of "SUPP" (e-invoice payment), both the *End to End Identification* or the *Creditor Reference* <CdtrRefInf/Ref> may be populated with the e-invoice payment ID (a textual value used to establish a link between the payment and the invoice issued by the seller. Used for the creditor's critical reconciliation information. This information element helps the seller to assign an incoming payment to the relevant payment process. Refer to https://github.com/A-NZ-PEPPOL/Guidance-documents). The e-invoice payment ID rule above is for domestic instructions only. Participants must not override the population of this element in an inbound cross-border transaction. Please refer to section 3.3.2 *Creditor Reference Information* for guidance on the population of messages to ATO or Services Australia.
Transaction Identification <TxId>	pacs.008 pacs.009 (CORE/COV)	The *Transaction Identification* <TxId> is a unique end-to-end identification, assigned by the first instructing agent, to unambiguously identify the transaction. It is passed on, unchanged, throughout the entire interbank chain. It can be used for reconciliation, tracking or to link tasks relating to the transaction at the interbank level. If no unique *Transaction Identification* can be generated, then the element is recommended by HVPS+ to be populated with a copy of the *Instruction Identification*. Usage: If it is present in the previous message in the payment chain (e.g., an inbound cross-border payment), it must be copied, unchanged, to the HVCS payment message.
Charge Bearer <ChrgBr>	pacs.004 pacs.008	Specifies which party/parties will bear the charges associated with the processing of the payment transaction. Available codes:

<table>
<tr>
<td></td>
<td></td>
<td>
<table>
<tr><th>Code</th><th>Name</th><th>Definition</th></tr>
<tr><td>CRED</td><td>Borne By creditor</td><td>All transaction charges are to be borne by the creditor.</td></tr>
<tr><td>DEBT</td><td>Borne By debtor</td><td>All transaction charges are to be borne by the debtor.</td></tr>
<tr><td>SHAR</td><td>Shared</td><td>In a credit transfer context, means that transaction charges on the sender side are to be borne by the debtor, transaction charges on the receiver side are to be borne by the creditor.

In a direct debit context, means that transaction charges on the sender side are to be borne by the creditor, transaction charges on the receiver side are to be borne by the debtor.</td></tr>
</table>
Note: In MT messaging, charges are requested using MTn91 messages. These will continue to be used as the equivalent ISO message, camt.106, is not yet available for use. [55]
</td>
</tr>
<tr>
<td>Service Level
<SvcLvl></td>
<td>pacs.008

pacs.009
(CORE/COV)</td>
<td>This element is retained for consistency with possible use in cross-border payments. Although generally not used in the HVCS, most gpi Participants will choose to populate this element with gpi service type identifiers.</td>
</tr>
<tr>
<td>Purpose

<CdtTrfTxInf/Purp>
></td>
<td>pacs.008

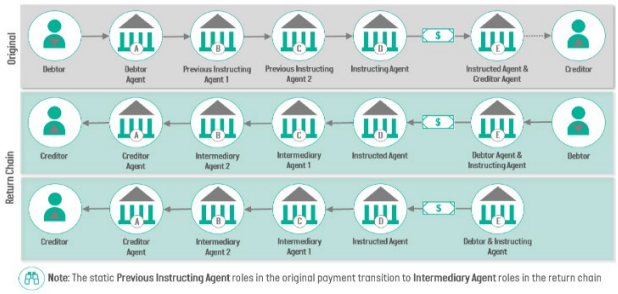
pacs.009
(CORE/COV)</td>
<td>The Purpose <Purp> element provides an underlying reason for the payment transaction. It is used by the end-customers, that is initiating party, (ultimate) debtor, (ultimate) creditor to provide information concerning the nature of the payment. Purpose is a content element, which is not used for processing by any of the agents involved in the payment chain.

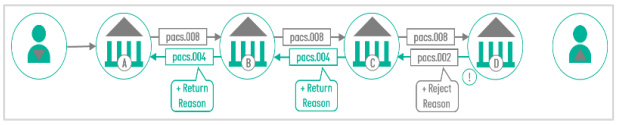
The use of Purpose codes has no impact on the processing of the payment, rather it is used to provide the ultimate creditor with information concerning the nature of the payment.

This element is different to Category Purpose <CtgyPurp>.

All valid Purpose codes can be used in the HVCS.</td>
</tr>
</table>

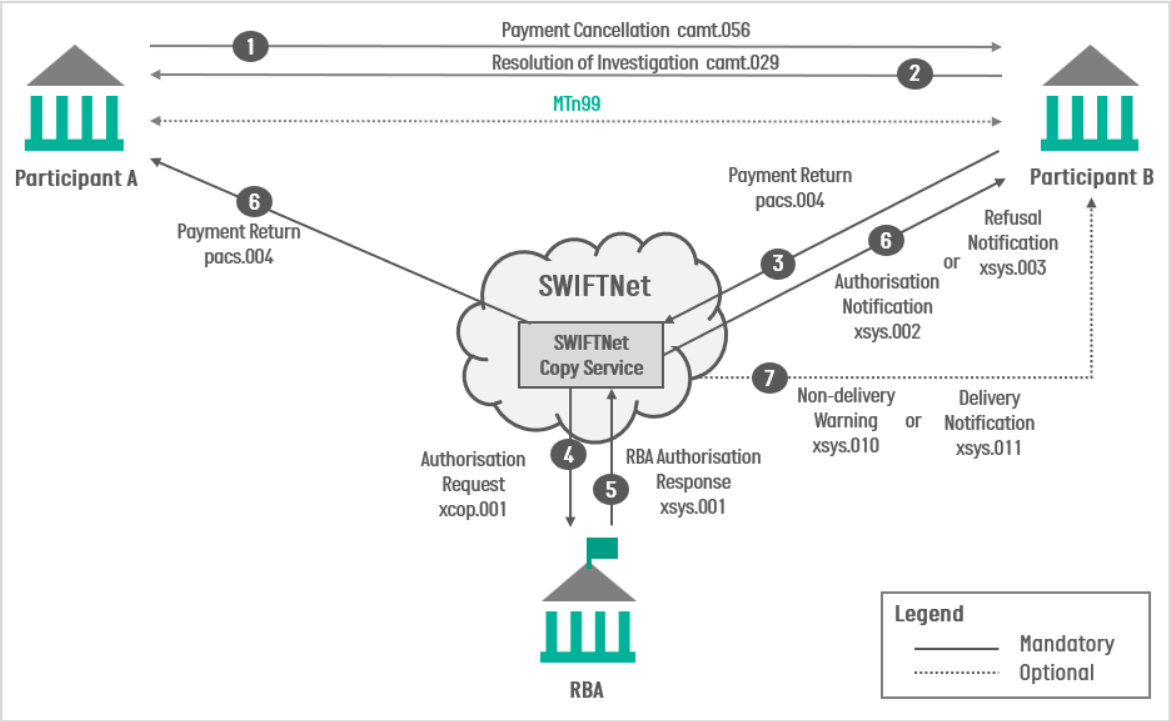
[55] Amended effective 23/9/24, version 4 r&p 001.24

Return Chain <TxInf/RtrChain>	pacs.004	Whereas the underlying payment message captures all the parties involved in the forward path of a payment, the mandatory *Return Chain* element captures all the parties involved in the return transaction.  In this element, the **roles** of the various parties change to reflect the fact the payment is now a *Payment Return. F*or example, the *Creditor Agent* of the underlying payment becomes the *Debtor Agent* of the *Payment Return*. If payment is made into the *Creditor* account in the original payment, the *Creditor* becomes the *Debtor* on the return chain (middle row). However, commonly the *Creditor Agent* is unable to apply funds to the *Creditor* account. In this case, the *Creditor Agent* becomes the *Debtor* on the return leg, as shown in the third row. As a rule of thumb, the *Debtor* in pacs.004 message reflects the account from which funds are being refunded.
Original Group Information/Original Message Identification <TxInf/OrgnlGpInf/OrgnlMsgId>	pacs.004	The *Original Message Identification* element contains the message identification from the BAH of the original payment message which the pacs.004 is returning. *Original Group Information* is mandatory in HVCS messaging but optional in FINPlus messaging. If it is not populated in a pacs.004 that originated from CBPR+, Intermediaries must ascertain it for the domestic leg of the transaction.
Original Group Information/Original Message Name Identification <TxInf/OrgnlGpInf/OrgnlMsgNmId>	pacs.004	The *Original Message Name Identification* element refers to the original message to which the return relates. e.g., if a pacs.008.001.xx was the original message, it would be included in the pacs.004. This element is mandatory and used by the RBA to apply RITS session validations. This element must include the full version name of the originating message (i.e., 'pacs.008.001.xx', 'pacs.009.001.xx', 'MT103' or 'MT202'). RITS will accept the current or previous version number of a pacs.008 or pacs.009 message in this element, to allow for the return of payments which were made prior to the adoption of a new message version number. If this element is not populated in a pacs.004 that originated from cross-border, the intermediary must ascertain it by reference back to the sender of the pacs.004 message.
Transaction Information/Original	pacs.004	The *Original Instruction Identification* is mandatory for domestic payments and optional for cross-border payments. It is

Instruction Identification <TxInf/OrgnlInstId>		populated with the *Instruction Identification* element in the original message which is being returned.
Transaction Information/Original End To End Identification <TxInf/OrgnlEndToEndId>	pacs.004	The *Original End to End Identification* element is populated with the *End To End Identification* element in the original message which is being returned.
Transaction Information/Original UETR <TxInf/OrgnlUETR>	pacs.004	The *Transaction Information* > *Original UETR* element would include the *UETR* of the payment message received. i.e., the same *UETR* is used on the return payment.
Original Transaction Reference <TxInf/OrgnlTxRef>	pacs.004	The *Original Transaction Reference* element includes detail from the *Original Message Name Identification*, e.g., in the below example, the *Debtor* of the original pacs.008 message.  *(Note: While not in scope for the HVCS, the pacs.002 is included in the above graphic to cover cross-border scenarios)*

3. Exception and Investigation (E&I) Messages (camt.xxx)

Payment returns may be the consequence of a payment cancellation requested by the payer Framework Participant or initiated by the payee Framework Participant as an unsolicited payment return. The ancillary query and investigation messages are designed to support investigation Case management in connection with payment cancellations or independently between a Case assigner and assignee. The diagram below describes the message flows.



It is important to note that ISO 20022 E&I messages will be transported within the ISO 20022 CUG.[56]

3.1 FI to FI Payment Cancellation Request (camt.056)[57]

(a) The FI to FI Payment Cancellation Request (camt.056) message is used to request the return of a payment, for example, in the case of a mistaken payment (payer error). When parties are ready to conduct exception and investigation messaging in MX, a solicited payment return must be initiated with the camt.056 and the requestor must include their investigation Case identifier within the 'Case/Identification' element within the camt.056 message. The camt.056 message is also referred to as the 'Request for a Payment Return' message.

3.2 Resolution of Investigation (camt.029)[58]

(a) The Resolution of Investigation (camt.029) message is used to either accept, reject, or provide a pending status for a FI to FI Payment Cancellation Request (camt.056) message. The receiver of the camt.056 message must resolve it with a camt.029 and must reference the original investigation identifier.

3.3 Element Population Principles (camt.xxx)

(a) The following element population principles outlines how key components within the camt.xxx message set are to be populated.

[56] Amended effective 23/9/24, version 4 r&p 001.24
[57] Amended effective 23/9/24, version 4 r&p 001.24
[58] Amended effective 23/9/24, version 4 r&p 001.24

#	Component	Principle
1	*Assignment* <Assgnmt>	(a) Always uniquely identifies the investigation message (identification), message sender (assigner), and message recipient (assignee).
2	*Case Identification* <Case/Id>	(a) Always the primary Case ID that is assigned by a Participant that creates the original Case. (b) Each Case must be represented with a single primary Case ID assigned by the original Case creator and may be associated with zero, one, or more secondary Case IDs assigned by their counterparty/counterparties. (c) *Case Identification* and *Case Creator* are represented as a pair of elements in each of the investigation messages.
3	*Case Creator* <Case/Cretr>	(a) The Participant that created the primary Case ID, as provided in the preceding component (*Case Identification*). (b) *Case Identification* and *Case Creator* are represented as a pair of elements in each of the investigation messages.

3.4 Guidance for Elements (camt.xxx)

Message	Component / Element	ISO Definition	Guidance
camt.056	*Case* <Case>	Identifies the investigation Case.	Additional guidance is not required.
	Case/ Identification <Case/Id>	Uniquely identifies the Case.	Case/Id assigned to this cancellation request. It represents either a new Case (where there is no existing Case being referenced) or an existing Case (as part of an ongoing investigation). This Case/Id is designated a primary case ID.
	Case/Creator <Case/Cretr>	The party that created the investigation Case.	Identifies the *Case Creator* that created the referenced investigation Case. Case/Id and *Case Creator* are paired elements in each of the Investigation messages.
	Reason <CxlRsnInf/Rsn/Cd>	Provides a reason selected from the reason code list	Although the full list of codes can be used, Participants must ensure that the cancellation request is made in accordance with these Procedures.
	Case/Reopen Case Indication <Case/ ReopCaseIndctn>	Indicates whether or not the Case was previously closed and is now re-opened.	Additional guidance is not required.
camt.029	*Resolved Case* <RslvdCase>	Identifies the resolved Case.	Additional guidance is not required.

	Confirmation <Status/Confirmation>	Indicates the status of the Case	The following codes are applicable: CNCL – Cancelled as per request PDCR – Pending cancellation request RJCR – Rejected cancellation request
	Reason <CxlStsRsnInf/Rsn/Cd>	Provides a reason selected from the reason code list	This element can be optionally populated in the case of a positive *Resolution of Investigation*, but must be provided if the *Status/Confirmation* = RJCR
	ResolvedCase/ Identification <RslvdCase/Id>	Uniquely identifies the Case.	Must contain the same information available under the Case/Id of the underlying camt.056. This Case/Id is designated a primary Case ID.
	Resolved Case/ Creator <RslvdCase/Cretr>	The party that created the investigation Case.	Must contain the same information available under the *Case/Creator* of the underlying camt.056.
	Case/Reopen Case Indication <Case/ ReopCaseIndctn>	Indicates whether or not the Case was previously closed and is now re-opened.	Not used in CBPR+.

4. SWIFTNet Y-Copy Message Set (xcop.001/xsys.xxx)

The HVCS Y-Copy message set includes the following SWIFTNet MX system messages:

(a) xcop.001 Partial Copy Message

(b) xsys.001 Y-Copy Authorisation or Refusal

(c) xsys.002 Y-Copy Authorisation Notification

(d) xsys.003 Y-Copy Refusal Notification

(e) xsys.010 Non-Delivery Warning

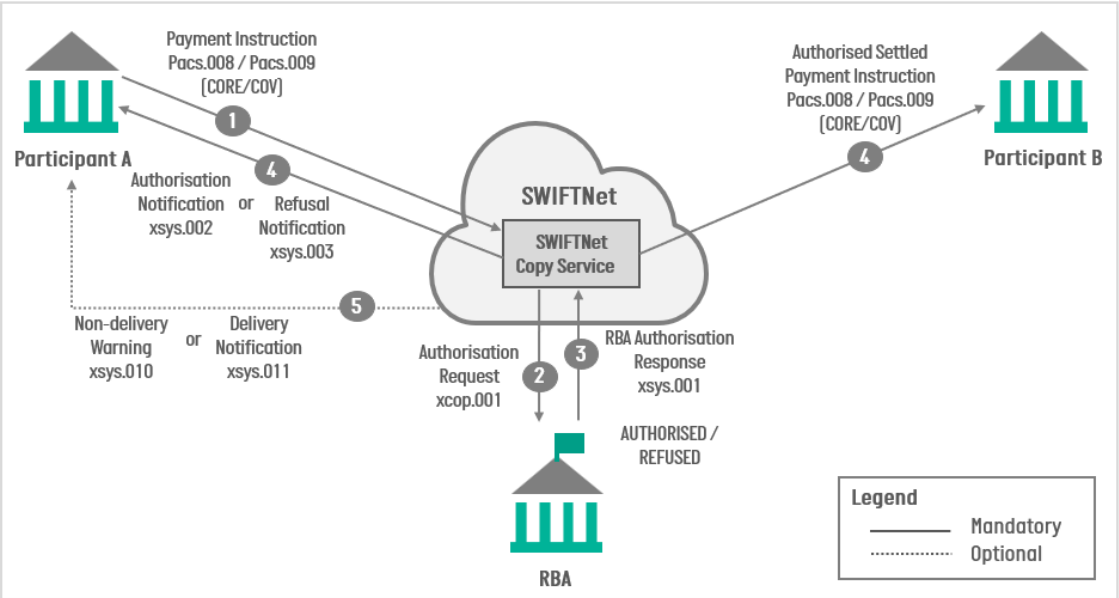
(f) xsys.011 Delivery Notification

All system messages are exchanged outside of the SWIFT PDS CUG.

The schemas for the HVCS xcop.001 and xsys.xxx system messages, together with some sample HVCS Y-Copy messages, can be found in the 'HVCS Community' section in SWIFT's MyStandards Readiness Portal.

The base xsys.xxx system messages together with samples are published in the SWIFT publication "SWIFTNet System Messages Guide".

Only system messages that relate to payment settlement are in scope for the HVCS, although a number of additional system messages can be used by Participants, notably, the xsys.015 Retrieval Request message. Full details of these messages are also contained in the "SWIFTNet System Messages Guide".



As illustrated in the diagram above:

(a) The HVCS operates on the SWIFTNet Copy Service, in a mandatory partial Y-Copy mode for the following message types; pacs.008, pacs.009 (CORE/COV) and pacs.004.

(b) In Y-Copy mode, SWIFT intercepts the pacs.008, pacs.009 (CORE/COV) and pacs.004 messages (flow 1) and copies prescribed fields from these payment messages to a copy destination, RBA (flow 2), using the xcop.001 message.

(c) SWIFT holds the payment message in a temporary queue until the RBA sends the appropriate authorisation or rejection (flow 3) using the xsys.001 message:

(i) If the RBA authorises the payment message, then SWIFT releases and forwards the pacs.008 / pacs.009 (CORE/COV) / pacs.004 message for delivery to the receiver. SWIFT notifies settlement to the sender using the xsys.002 message (flow 4) and for the receiver, includes the settlement information in the SWIFTNet Header of the payment message (flow 4).

(d) As part of the normal InterAct features, the sender can request that SWIFT monitors the delivery of sent messages (flow 5). In this case, SWIFT returns an xsys.010 Non-Delivery Warning message or an xsys.011 Delivery Notification message, to the sender, as appropriate. These notifications are based on the delivery of the original payment message to its receiver, and not on the delivery of the copy to RBA.

(e) Further information is provided in the SWIFT publications "SWIFTNet Service Description", "SWIFTNet Messaging Operations Guide", "SWIFTNet System Messages Guide", and "SWIFTNet Vendor Interface Specifications".

4.1 Partial Copy Message (xcop.001)

(a) The xcop.001 message is sent from the SWIFTNet InterAct partial Y-Copy to the third party (RITS) when triggered by a payment message. The xcop.001 for RBA comprises the data elements listed in the table below. The table also shows whether the element is optional or mandatory in the xcop.001 message and in the underlying payment message.

Name	Element	xcop M/O	HVCS M/O
head.001 (Business Application Header	**<AppHdr> - Entire Structure**	**O**	**M**
pacs.008 (FI To FI Customer Credit Transfer)	**<FIToFICstmrCdtTrf>**		
Clearing System Code	<ClrSys/Cd>	O	M
Instruction Identification	<InstrId>	O	M
End To End Identification	<EndToEndId>	M	M
Transaction Identification	<TxId>	O	O
UETR	<UETR>	O	M
Payment Type Information	<PmtTpInf> - Entire structure	O	O
Interbank Settlement Amount	<IntrBkSttlmAmt + Ccy>	M	M
Interbank Settlement Date	<IntrBkSttlmDt>	O	M
Instructing Agent BIC	<InstgAgt>	O	M
Instructed Agent BIC	<InstdAgt>	O	M
Category Purpose	<CtgyPurp>	O	O
pacs.009 (Financial Institution Credit Transfer)	**<FICdtTrf>**		
Clearing System	<ClrSys/Cd>	O	M
Instruction Identification	<InstrId>	O	M
End To End Identification	<EndToEndId>	M	M
Transaction Identification	<TxId>	O	O
UETR	<UETR>	O	M
Payment Type Information	<PmtTpInf> - Entire structure	O	O
Interbank Settlement Amount	<IntrBkSttlmAmt + Ccy>	M	M

Interbank Settlement Date	<IntrBkSttlmDt>	O	M
Instructing Agent BIC	<InstgAgt>	O	M
Instructed Agent BIC	<InstdAgt>	O	M
Category Purpose	<CtgyPurp>	O	O
pacs.004 (Payment Return)	**<PmtRtr>**		
Clearing System	<ClrSys/Cd>	O	M
OriginalGroupInformation	<OrgnlGrpInf> - Entire structure	O	O
Original Message Name Identification	<OrgnlMsgNmId>	O	O
Original End To End Identification	<OrgnlEndToEndId>	O	M
Return Identification	<RtrId>	O	M
Original Instruction Identification	<OrgnlInstrId>	O	O
Original Transaction Identification	<OrgnlTxId>	O	O
Original UETR	<OrgnlUETR>	O	M
Returned Interbank Settlement Amount	<IntrBkSttlmAmt + Ccy)>	O	M
Interbank Settlement Date	<IntrBkSttlmDt>	O	M
Instructing Agent BIC	<InstgAgt>	O	M
Instructed Agent BIC	<InstdAgt>	O	M
Original Category Purpose	<CtgyPurp>	O	O

4.2 Y-Copy Authorisation or Refusal (xsys.001)

(a) When the RBA authorises the settlement transaction for release to the receiver following settlement, the RBA will populate both of the following xsys.001 message components:

(i) *ThirdPartyToSenderInformation* (specific settlement data for the message sender); and

(ii) *ThirdPartyToReceiverInformation* (specific *settlement* data for the message recipient)

(b) The RBA will use these fields to convey settlement information related to the authorisation (such as actual settlement date/time and amount, RITS Allocation balance, etc).

(c) SWIFT includes this information in the Y-Copy authorisation notification (xsys.002 message) that it sends to the pacs.008 / pacs.009 (CORE/COV) / pacs.004 sender,

and includes this settlement information in the SWIFTNet Header of the authorised pacs.008 / pacs.009 (CORE/COV) / pacs.004 message forwarded to the receiver.

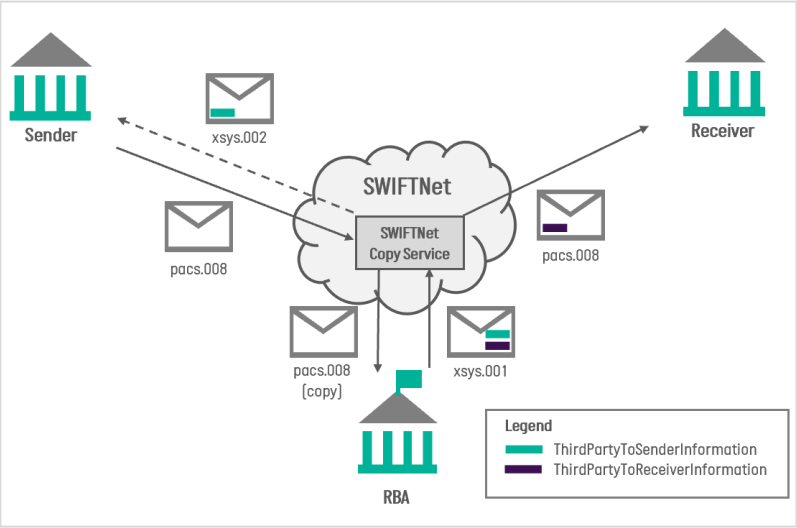
(d) When the RBA refuses the settlement transaction, the RBA will populate the following xsys.001 message component:

(i) *ThirdPartyRefusalReason* (specific refusal data for the message sender)

(e) SWIFT does not release to the intended recipient a refused settlement request. The message sender is sent notice of the refusal in the Y-Copy refusal notification (xsys.003 message).

(f) Across settlement, no change is made to the payment message itself (BAH and underlying pacs.008 / pacs.009 (CORE/COV) / pacs.004), this payload remains identical between the sender and the receiver. Information concerning successful settlement is conveyed in a system message (xsys.002) sent by SWIFT back to the sender. For the receiver, this information is incorporated in a dedicated information block in the SWIFTNet Header of the payment message.

xsys.001 (Y-Copy Authorisation or Refusal)	Definition
Authorisation Status	Indicates whether settlement of the pacs.008 / pacs.009 / pacs.004 message is Authorised or Refused.
Store And Forward Reference	*Internal Service Reference*
Copy Store And Forward Reference	*Internal Service Reference*
Service	*Internal Service Reference*
Third Party To Receiver Information	RBA data that is forwarded to the receiver (XML structure specific to HVCS): - Date/Time Transaction was settled (in local) - Interbank Settlement Amount - ESA Balance
Third Party To Sender Information	RBA data that is returned to the sender (XML structure specific to HVCS): - Date/Time Transaction was settled (in local) - Date/Time instruction received within RITS - Interbank Settlement Amount - ESA Balance
Third Party Refusal Reason	In the case of refusal, the RBA will provide a reason code
Signature Value	*For non-repudiation purposes*



4.3 Y-Copy Authorisation Notification (xsys.002)

(a) The Y-Copy Authorisation Notification is generated by SWIFTNet to notify the Sender (Debtor Agent) that a pacs.008 / pacs.009 (CORE/COV) / pacs.004 message has been authorised by RITS - an xsys.001 with AuthstnSts equal to 'Authorised'.

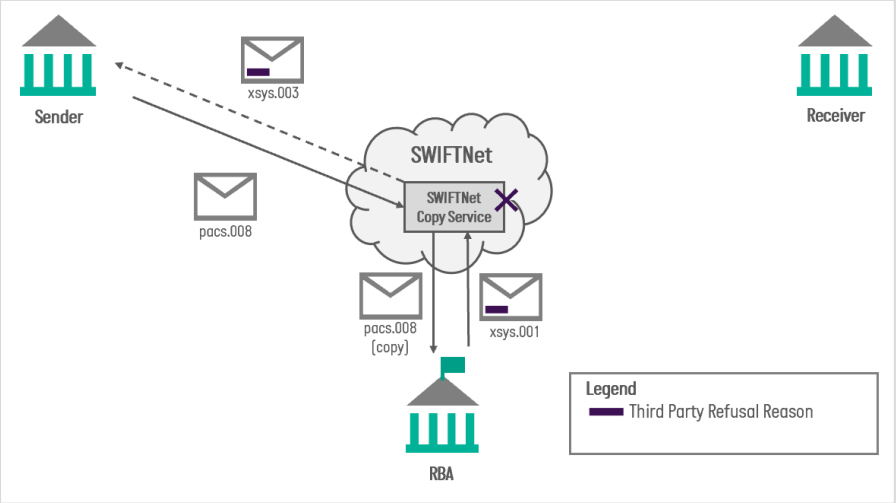
(b) Payment release information is conveyed to the Sender in the *ThirdPartyToSenderInformation* element of the xsys.002 message.

(c) The HVCS Y-Copy will generate either an Authorisation Notification (xsys.002) or Refusal Notification (xsys.003) in response to each pacs.008, pacs.009 (CORE/COV) or pacs.004 sent for clearing, so the sender will always receive a message confirming clearing status of each message.

4.4 Y-Copy Refusal Notification (xsys.003)

(a) The Y-Copy Refusal Notification is a system message generated by SWIFTNet to alert the Sender (Debtor Agent) that a pacs.008 / pacs.009 (CORE/COV) / pacs.004 message has been refused by RITS - an xsys.001 with *AuthstnSts* equal to 'refused'.

(b) This xsys.003 message contains the *ThirdPartyRefusalReason*, which provides further information about the refusal (see Third Party Refusal reason codes below).



4.5 Linking xsys.002/3 to the original pacs.xxx message

(a) Participants can link the original payment message to the relevant xsys.002 or xsys.003 message in one of two ways:

(i) The messaging interface adds the SnFRef to the outgoing payment and this is carried through to the corresponding ACK and xsys.002/3 message. However, as the SnFRef is not present in the back office, it must be used in conjunction with another element which is common to both the SWIFTNet Header and the message body to reconcile the messages.

(ii) Participants may configure their messaging interface to carry a unique element from the message body (for example Instruction

Identification/Return Identification) to User Reference in the SWIFTNet Header. As User Reference is returned in the xsys.002/3 message as Request Reference, it can link the original payment to the xsys.002/3. If using this method, participants must take care when reconciling message retransmissions, as they will not carry a unique Instruction Identification/Return Identification.

4.6 Non-Delivery Warning (xsys.010)

(a) The SWIFTNet Y-Copy service generates *the Non-Delivery Warning* (xsys.010) when a message (pacs.008 / pacs.009 (CORE/COV) / pacs.004) is considered to be overdue (not delivered within the time frame specified by the sender Participant).

(b) The xsys.010 message is optional.[59]

(c) A message sender can select the *Non-Delivery Warning* feature when sending a message indicating in the SWIFTNet Header the period of time after which they require notification if the message has not been delivered. SWIFT tries to deliver the message as normal, and if successful does not notify the sender. Performed on a per-message basis. The period of time can be between 5 minutes and 1 day.

(d) Members should refer to the SWIFTNet system message specification for the additional xsys.010 fields and example of the XML structure.

(e) Status codes:

(i) *PendingAuthorisation* (The message is not yet authorised by the RBA).

(ii) *AuthorisedPendingDelivery* (The *message* is authorised by RBA, but not yet delivered.

4.7 Delivery Notification (xsys.011)

(a) The *Delivery Notification* message is an optional system message that indicates that a message for which a delivery notification is requested, has been successfully delivered.

(b) The *Delivery Notification* is reconciled with the InterAct request to which it applies.

(c) The xsys.011 message is optional.[60]

(d) A sender of the message may explicitly request the *Delivery Notification*. SWIFTNet generates a *Delivery Notification* when it receives the technical delivery acknowledgement from the receiver's interface.

(e) Members should refer to the SWIFTNet system message specification for the additional xsys.011 fields and example of the XML structure.

[59] Amended effective 23/9/24, version 4 r&p 001.24
[60] Amended effective 23/9/24, version 4 r&p 001.24

(f) The xsys.010 and xsys.011 messages are based on the delivery of the original message to its receiver, and not on the delivery of a copy to the copy destination.

4.8 Third Party Refusal Reason Codes (xsys.001 and xsys.003)

(a) The table below lists all of RITS's reason codes if settlement of a payment is unsuccessful, together with some examples illustrating when these codes may be used. The reason codes will be included in the xsys.001 (Authorisation Response) message, sent from the RBA to the SWIFT Y-Copy service. This reason code, used in the xsys.001, will then be passed onto the sending Framework Participant within the xsys.003 (Refusal Notification) message. If RITS identifies an issue with the xcop.001 message, then validation will immediately cease at that point, with the relevant reason code provided to the SWIFT Y-Copy service.

Reason Code	Description	Example Validation failures
AC06	*Blocked Account*	The debtor or creditor is not active or has been suspended in RITS.
AG03	*Transaction Not Supported*	Either the debtor or creditor has not agreed to operate in the Evening Settlement Session.
AM12	*Invalid Amount*	The Amount is more than $9,999,999,999.99 or does not contain exactly two fractional digits.
CURR	*Incorrect Currency*	The currency is not AUD.
CUST	*Requested By Customer*	The sending Participant recalled the message before settlement (e.g. via the RITS Automated Information Facility).
DT01	*Interbank Settlement Date Invalid*	The *Interbank Settlement Date* is before the current date or more than five business days post the current date.
DUPL	*Duplicate Payment*	The payment is a duplicate of another payment within 15 calendar days since first being used.
ED05	*Settlement Failed*	The message is removed by RITS as unsettled at the end of the day.
RC05	*Invalid BIC Identifier*	The debtor or creditor BIC is invalid according to RITS and either: • The sender/receiver BICs in the SWIFTNet Header do not match the to/from elements in the Business Application Header; or • The From/To BICs in the Business Application Header do not match the instructing/instructed agent elements of the message body.
TD03	*Incorrect File Structure*	The message format standards have not been met, for example: • The message does not conform to the xcop.001 XSD.

		• The Message Definition Identifier in the Business Application Header does not equal either a pacs.008, pacs.009 (CORE/COV) or pacs.004. • The Business Service field in the Business Application Header is invalid. • The *Clearing System Code* is invalid.
TM01	*Invalid Cut Off Time*	The payment is received outside of a valid RITS session time for that payment, including national public holidays and weekends.

5. Customer to FI / FI to Customer (CFI) messages [Deleted][61]

6. Message Processing – Character Set

(a) All HVCS ISO 20022 message elements which are defined (by data type) as text are restricted to the character set: a-z A-Z 0-9 / - ? : ( ) . , ' +.

(b) The following special characters: !#$%&'*=?^_`{|}~ "();<>@[\] are additionally allowed in:

(i) All party (agents and non-agents) *Name and Address* elements;

(ii) The *Related Remittance* Information <RltdRmtInf> element; and

(iii) The *Remittance Information* <RmtInf> element.

(c) Non-Latin characters (including Mandarin, Cantonese, Arabic, Cyrillic characters etc) are not to be used. Translation of these, or any special character (noting exceptions above) will be represented by a (full stop).

(d) Participants needing to exchange information containing (for example) Chinese alphabet characters will need to make arrangements to do so outside the ISO 20022 CUG. For example, inbound messages using non-Latin characters could be exchanged via FileAct (forgoing SWIFT Network validation) on SWIFTNet, or via a channel outside SWIFT. Participants entering into this type of arrangement must ensure their IFTI reporting obligations are not compromised.

(e) Emojis are not permitted in the HVCS.

(f) In relation to message content generally, Participants must keep up to date with, and follow, current industry guidelines on safeguards against abuse in payment messages.

7. Message Processing – Structured Data

The move to structured data in ISO 20022 format payments will increase the quality of data available for screening and identification of customer behaviour, which can be used for fraud prevention purposes. The use of dedicated elements in the ISO 20022 schema will remove ambiguity around data mapping to the schema. Participants must ensure their customer data set is current and complete to be able to realise the benefits of structured data.

[61] Deleted effective 23/9/24, version 4 r&p 001.24

The following outlines the agreed approach for the adoption of structured data (across both structured remittance and name and address elements):

(a) There will be no near-term mandate to use structured remittance or structured name and address.

(b) Use of structured remittance and name and address is encouraged.[62]

(c) Structured data is allowed for in the message specification, and Participants are free to use it if they wish. For that reason, all Participants' systems must be able to receive and process messages containing structured name and address and structured remittance.[63]

7.1 Remittance Information[64]

(a) The guidance in this section applies to remittance data in all HVCS messages, including the pacs.008, pacs.009 (CORE/COV) and pacs.004.

(b) Structured and Unstructured Remittance Elements:

(i) Use of structured data is recommended, although use of unstructured data remains available. Unstructured remittance information can be contained in a CBPR+ payment and should be passed on to the creditor/ultimate creditor. Typically, structured remittance information is more applicable for reconciliation of invoices as noted in the definition in the MUGs "*Information supplied to enable the matching/reconciliation of an entry with the items that the payment is intended to settle, such as commercial invoices in an accounts' receivable system, in a structured form*". Unstructured remittance information is used for other non-invoice related payments where there may be no references to include.

(ii) Any unstructured, freeform text must only be populated in a *Remittance Information/Unstructured* <RmtInf/Ustrd> element, noting the two cross-element rules (as per HVPS+ and CBPR+):

(A) *Remittance Information/Unstructured* <RmtInf/Ustrd> and *Remittance Information/Structured* <RmtInf/Strd> are mutually exclusive and both may be absent.

(B) *Related Remittance Information and Remittance Information* are mutually exclusive (noting these fields are not mutually exclusive in NPP).

(iii) The HVCS pacs.008 *Remittance Information/Unstructured* <RmtInf/Ustrd> allows 1x140 characters (to align with HVPS+ and CBPR+).

(iv) The *Additional Remittance Information* <RmtInf/Strd/AddtlRmtInf> element should only be used when the *Remittance Information/Structured* elements

[62] Amended effective 23/9/24, version 4 r&p 001.24
[63] Amended effective 23/9/24, version 4 r&p 001.24
[64] Amended effective 23/9/24, version 4 r&p 001.24

are used and to supplement data already populated in other *Remittance Information/Structured* <RmtInf/Strd> elements.

(v) *Remittance Information/Structured* <RmtInf/Strd> elements are currently unbounded; however, population must be limited to 9,000 characters to align with CBPR+. That is, 9000 characters, excluding the tags (i.e., 9000 characters of business data) and including 3x140 characters in the *Additional Remittance Information* <AddtlRmtInf> element.

(c) Structured Invoice Information

(i) If payments are made on behalf of corporates who are paying multiple invoices in the same remittance, invoice numbers should be populated in *Referred Document Information* <RmtInf/Strd/RfrdDocInf>, which is a repeatable component.

(ii) In order to maintain consistency domestically and with CBPR+, structured invoice information should be populated as follows:

Level	ISO 20022 Tag	Element Description	Notes	Example
6	<RfrdDocInf>	Referred Document Information	If required, information about the identification and content of the referred document must be provided in this component	
7	<Tp>	Type	Specifies the type of referred document	
8	<CdOrPrtry>	Code Or Proprietary	Either a code or a proprietary identification can be used to specify the document type	
9	<Cd>	Code	Choose a code from list in the MUGs, for example, Commercial Invoice (CINV)	CINV
9	<Prtry>	Proprietary	If an appropriate Code cannot be found to identify the document, it can be entered here	-
7	<Nb>	Number	Unique and unambiguous identification of the referred document	AS0009876
7	<Dt>	Related Date	Date associated with the referred document	2022-08-27

(iii) Note: that separate rules apply to e-invoicing. Please refer to the following section Creditor Reference Information below.

(d) Creditor Reference Information

(i) When structured remittance information is used, the *Creditor Reference Information* <CdtrRefInf> component should be used to provide reference information from the creditor. Any other remittance information must be mapped to another appropriate element within *Remittance Information/Structured* <RmtInf/Strd>.

(ii) For domestic payment transactions assigned a *Category Purpose* of "SUPP" (PEPPOL e-invoice payment), End to End Identification or Creditor Reference Information may be populated with the e-invoice payment ID. Participants must not override the population of this element in an inbound cross-border transaction. Please refer to Section 2.3.4 Guidance for Elements (pacs.008 / pacs.009 (COR/COV) / pacs.004) End to End Identification for more information about this process.

(iii) Payments to ATO or Services Australia must provide an EFT code or reference number which can be used by the creditor to identify and automatically reconcile the payment. In pacs.008 or pacs.009 messages, this information must be populated in either:[65]

(A) The structured element Creditor Reference Information *<CdtrRefInf/Ref>; or*

(B) The unstructured element Remittance information Unstructured *<RmtInf/Ustrd>*; or

(C) End to End Identification *<EndToEndId>.*

(iv) In addition, ATO payments may be optionally populated with TAXS in the Category Purpose Code. There is no Category Purpose Code associated with Services Australia payments.

7.2 Structured Name and Address[66]

(a) This section provides market practice guidelines for the use of structured name and address elements in all HVCS messages, including the pacs.008, pacs.009 (CORE/COV) and pacs.004 messages.

(b) Structured Address in ISO 20022

(iv) ISO 20022 provides structured and granular data for the identification of a party in the name and address components.[67]

(v) Domestically, Participants may need to obtain additional customer details to allow the structured name and address to be mapped into the ISO 20022 schema. It is recommended that Participants review their processes relating to customer data to ensure they capture all schema elements listed below. It is anticipated that, for some Participants, collating this level of

[65] Amended effective 23/9/24, version 4 r&p 001.24
[66] Amended effective 23/9/24, version 4 r&p 001.24
[67] Amended effective 23/4/24, version 4 r&p 001.24

detail for all customers will take time. Participants should consider that the use of structured name and address will become mandatory in the future.

(vi) The table below indicates best practice in the use of structured address in Australia. The elements *Town Name* and *Country* are marked as 'Mandatory', which is consistent with CBPR+, whereas population of elements marked as 'Recommended' is deemed best practice when originating payment messages in Australia. This means that Intermediary Framework Participants do not need to seek additional address information in order to comply with HVCS rules when on-sending a payment that has originated from overseas.

Level	ISO 20022 Tag	Element Description	Definition	Universal Post Union (UPU) Element	Usage in HVCS (If Structured Address is Used)
2	<Dbtr>	Debtor			
3	<Nm>	Name [68]	Name by which a party is known, and which is usually used to identify that party.	Addressee	Recommended
3	<PstlAdr>	**Postal Address**	Information that locates and identifies a specific address, as defined by postal services.		
4	<Dept>	Department	Identification of a division of a large organisation or building.	Department	Optional [69]
4	<SubDept>	Sub Department	Identification of a sub-division of a large organisation or building.	Sub Department	Optional[5]
4	<StrtNm>	Street Name	Name of a street or thoroughfare.	Street	Recommended
4	<BldgNb>	Building Number	Number that identifies the position of a building on a street.	No.	Recommended
4	<BldgNm>	Building Name	Name of the building or house.	Building name	Optional[5]
4	<Flr>	Floor	Floor or storey within a building.	Floor	Conditional [70]

[68] The Full Legal Account Name (FLAN) is not required when populating the Debtor/Name element of payment messages, however, Participants may choose to use the FLAN if preferred. Participants must also remain mindful of their IFTI reporting obligations to ensure the required information is included in inbound and outbound cross- border transactions prior to reporting to AUSTRAC.

[69] Usage is rare (depends on whether it is present in the KYC system).

[70] Mandatory where multiple different entities reside on different floors in the same building

4	<PstBx>	Post Box	Numbered box in a post office, assigned to a person or organisation, where letters are kept until called for.	P.O. Box Number	Conditional [71]
4	<Room>	Room	Room	Apartment No.	Conditional [72]
4	<PstCd>	Post Code	Identifier consisting of a group of letters and/or numbers that is added to a postal address to assist the sorting of mail.	Postcode	Recommended
4	<TwnNm>	Town Name	Also known as Suburb. Name of a built-up area, with defined boundaries, and a local government. This should not include the name of the city within which the Suburb is located. [73]	Locality	Mandatory
4	<TwnLctnNm>	Town Location Name	Specific location name within the town.	Sub-locality	Not applicable / shouldn't be used
4	<DstrctNm>	District Name	Identifies a subdivision within a country sub-division.	N/A	Not applicable / shouldn't be used
4	<CtrySubDvsn>	Country Subdivision	Identifies a subdivision of a country such as state, region, county.	State	Recommended
4	<Ctry>	Country	Nation with its own government.	Country	Mandatory

(vii) Further to the above, Participants must note the following guidelines:

(A) If *Postal Address* <PstlAdr> is present, then *Name* <Nm> is mandatory.

(B) If *Postal Address* <PstlAdr> is used and if *Address Line* <AdrLine> is present, then all other optional elements in *Postal Address* <PstlAdr> must be absent.

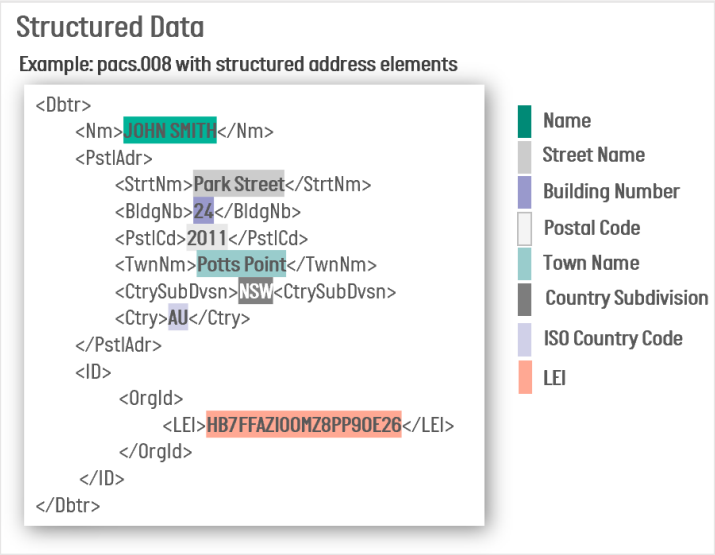
(C) If *Postal Address* <PstlAdr> is used and if *Address Line* <AdrLine> is absent, then *Country* <Ctry> and *Town Name* <TwnNm> must be present.

(viii) Below is an example of ISO 20022 pacs.008 use of the structured name and address elements:

[71] Exclusive use is considered non-compliant from a payment perspective based on Australian legislation. The use of the PO Box <PstBx> element is not recommended, given potential sanctions screening issues this may present (as per Wolfsberg Group – Payment Transparency Standards). AUSTRAC's Anti-Money Laundering / Counter Terror Financing (AML/CTF) Act also states that the primary address cannot be a PO Box. However, it can be used exclusively in structured data as long as one additional identifier is provided

[72] Mandatory where the residential address is an apartment.

[73] For example, correct use would be 300 Barangaroo Ave, Barangaroo NSW 2000, Australia. Incorrect use would be 300 Barangaroo Ave, Barangaroo, Sydney NSW 2000, Australia.



8. Distinguished Name

The BIC alone is no longer used to define the way messages are addressed in the network. MX messaging use the ISO standard naming convention of DN to uniquely identify the destination (responder DN) or source (requestor DN) of a message.

The DN is comprised of segments in up to 4 levels:

(a) Level 1 (the root level) is mandatory and always **o=swift.**

(b) Level 2(institution level) is mandatory, must be a published BIC8, and is designated by **o=**, e.g., **o=ptspauaa.**

(c) Level 3 (organisational unit **ou=**) is optional and can have multiple instances. A typical use of the **ou=** segment is to define the 3-character Branch Identifier extension that makes up a BIC11.

(d) Level 4 (common name **cn=**); **cn=** is a level 4 segment when a level 3 segment is present, but **cn=** can also be a level 3 segment. **cn=** can have any value and can be used to further identify message addressing.

DNs are comma delimited and always shown in the sequence of highest level through to mandatory levels 2 and 1. For example:

(a) A3-Level DN: ou=xxx,o=ptspauaa,o=swift

(b) A4-Level DN: cn=qwerty,ou=xxx,o=ptspauaa,o=swift

For the HVCS production service, DNs must consist of 3 levels with the second level consisting of an 8-character published BIC and the third level being a 3-character branch code (or xxx if no branch code is specified). Hence, Participants will be able to derive the production DNs of other Participants from the BIC register which is maintained by the Company.

As described below, Pilot DNs, may extend to 4 levels to provide Participants with the flexibility to route to multiple test environments. The first 3 levels of the Pilot DN must be structured in the same way as the live DN as described above, with an additional level added if Participants require more

granularity in the segregation of test traffic. The same 3 level DN may be used for Pilot DN and live operations.

When applying for membership of the HVCS pilot and production CUGs using the SWIFT subscription e-form, Participants will be required to specify the DNs they intend to use. Details of this process are provided by the Company when on-boarding new Framework Participants.

SWIFT will not validate the structure of DNs used outside of the FINplus service, so Participants must ensure they following DN formatting rules set out in the SWIFT publication "SWIFT.com Knowledge Centre SWIFTNet Naming and Addressing Guide".

9. BIC/BSB Usage

9.1 BIC Validation and Consistency Requirements

(a) The BIC element is a mandatory component in the SWIFTNet Header, BAH and message payload. The BIC8 used in all three of these message components must be identical and published in the "SWIFTNet Directory". Note that the 3-character Branch Identifier may be published or unpublished.

(b) SWIFT will undertake central validation to ensure that the BIC8 used in the SWIFTNet Header and BAH are published but will not conduct consistency checking that the two elements are identical.

(c) Consistency checking of the BIC8 in payment messages will be undertaken within RITS as follows:

(d) The BIC8 in the *Sender DN* and *Receiver DN* of the SWIFTNet Header must be identical to the corresponding BIC8 in the *From* and *To* elements of the BAH; and

(e) The BIC in the in the *To* and *From* elements of the BAH must be identical to the corresponding BIC in the *Instructed Agent* and *Instructing Agent* of the message payload.

(f) This means that, although messages may pass SWIFT validation, they will be rejected by RITS if failing BIC consistency validation. In this situation, the reason code provided in the xsys.003 message will be RC05 (*Invalid BIC Identifier*).

(g) The only situation where the BIC elements do not need to be identical is when the *Copy/Duplicate* indicator is set to *Copy*.

9.2 Segregation of Test and Production Messaging[74]

(a) The MX test (pilot) service requires use of a published BIC8. Use of a DN ensures messages are routed to the correct environment.[75]

(b) Participants must ensure that their processes and systems have sufficient protections to ensure test messages using live BICs do not escape into production, particularly when making technical changes, such as routing changes.

[74] Amended effective 23/9/24, version 4 r&p 001.24
[75] Amended effective 23/9/24, version 4 r&p 001.24

(c) The BIC is combined with the *Service Name* in the SWIFTNet Header (Network Header) of an InterAct message, to ensure correct addressing and separation of test and production traffic.

9.3 Using BIC and BSB elements in MX messaging

(a) The BIC and BSB are used as identifiers in the population of FI (agent) elements and debtor and creditor elements in MX messaging for the purposes of routing and clearing payments.

(b) It is mandatory to include the BSB together with the account number in domestic MX messaging within the HVCS, although it is optional in payments that have originated from cross-border. If the BSB is not known or not identical between data elements the creditor agent may:

(i) Clear the payment using the account number alone, if it is unique;

(ii) Return the payment; or

(iii) Seek clarification from the sender.

(c) It will ultimately be up to the receiving agent to determine whether the account is enabled to receive HVCS payments.

(d) Participants should populate these elements in all pacs.xxx messages as described below.

Purpose	Element	Guidance
These elements are used to identify the debtor and creditor account details. Please refer to the following section for a detailed explanation of the valid combination of elements when originating a payment message domestically.	*Creditor Account Identification* *<CdtrAcct/Id/Othr/Id>* *Debtor Account Identification* *<DbtrAcct/Id/Othr/Id>*	This is a mandatory element when including the creditor or debtor's account identification when other than IBAN. In Australia, a bank account is uniquely identified by the 6-digit BSB followed by the account number (usually up to 9 digits). The BSB must be provided in domestic payment messaging, but can be omitted if the payment has originated from overseas.
	Scheme Name *<CdtrAcct/Id/Othr SchmeNm/Cd>* *<DbtrAcct/Id/Othr SchmeNm/Cd>*	The *Scheme Name* is an optional element for both the debtor account and creditor account. The code value 'BBAN' may be used to indicate that the account identification is a basic bank account number.
	Issuer	*Issuer* is an optional element for both the debtor account and creditor account. If present, for an Australian account, it must be identical to the 6-digit BSB and

	<CdtrAcct/Id/Othr/Issr> *<DbtrAcct/Id/Othr/Issr>*	may be extracted from the account identifier (if BSB is present).
These elements are used in the identification of Financial Institutions: 1) For domestic payments, either BIC or (Name and Postal Address) or ClearingSystemMemberIdentification must be present and any can be present. Other elements remain optional. 2) For cross-border payments: - if BIC is present, then (Name & Postal Address) is NOT allowed (ClearingSystemMemberIdentification and LEI may complement) In case of conflicting information, the BIC will always take precedence. - If BIC is absent, (Name & Postal Address) or ClearingSystemMemberIdentification must be present and both are allowed together. 3) "Instructing/ Instructed Agents" must be identified with a BIC - Clearing System Members Identification and LEI are optional.	BICFI *<FinInstnId/BICFI>*	When used, must be populated with a published BIC8. The 3-character Branch Identifier may also be appended, making a total of 11 characters, and this may be published or unpublished.
	Clearing System Identification *<FinInstnId/ClrSysMmbId/ClrSysId/Cd>*	When used in Australia, the *Clearing System Identification* is always the 5 characters 'AUBSB'.
	Member Identification *<FinInstnId/ClrSysMmbId/MmbId>*	When used, this is the 6-digit BSB

(e) In MX messaging, the *Creditor Account* and *Debtor Account* components are optional and there are a number of valid combinations that can be used to describe creditor/debtor information, including the account number.

(f) The table below shows the valid combinations that can be used to describe creditor information when originating payment messages domestically. The same options also apply when describing debtor information. It is not mandatory to include address or account number in CBPR+ messaging and therefore they may be absent in the domestic leg of a cross-border payment.

Option	Valid Combination	XML Path	Comments
1	Name + AddressLine + Account	From the Creditor component: Cdtr/Nm Cdtr/PstlAdr/AdrLine And From the Creditor Account component: CdtrAcct/Id/Othr/Id Or From the Creditor Account component: CdtrAcct/Id/Othr/Id CdtrAcct/Id/Othr/SchmeNm/Cd CdtrAcct/Id/Othr/Issr	When on-sending a payment that has originated from cross-border, *AddressLine* may be left blank if an address is not provided. *Creditor Account* is populated in one of 2 ways: • *Id* is populated with the account number and BSB is prefixed as the first 6 digits • *Id* is populated with the account number and BSB separately populated in *Issuer*. If *Issuer* is used, *Scheme* should also be populated with BBAN The BSB may be absent in cross-border payments.
2	Name + AddressLine + Id	From the Creditor component: Cdtr/Nm Cdtr/PstlAdr/AdrLine And Cdtr/Id/OrgId/Othr/Id Or Cdtr/Id/OrgId/Othr/Id Cdtr/Id/OrgId/Othr/SchmeNm/Cd Cdtr/Id/OrgId/Othr/Issr Or Cdtr/Id/PrvtId/Othr/Id	When on-sending a payment that has originated from cross-border, *AddressLine* may be left blank if an address is not provided. *OrgId* or *PvtId* are used to uniquely identify an organisation or person, respectively. *OrgId* is populated with the account number in one of 2 ways: • *Id* is populated with the account number and BSB is prefixed as the first 6 digits • *Id* is populated with the account number and BSB is separately populated in *Issuer*. If *Issuer* is used, *Scheme* should also be populated with BANK. Cross-border payments may contain an alternative form of party identification in *Id.*
3	Name + TownName + Country + Account	From the Creditor component: Cdtr/Nm Cdtr/PstlAdr/TwnNm Cdtr/PstlAdr/Ctry From the Creditor Account component: CdtrAcct/Id/Othr/Id	If using structured Postal Address, *TownName* + *Country* must be present. This aligns with CBPR+ rules. It is recommended to add *Postal Code* although it is optional. The *Creditor Account* may be populated with the account number prefixed with the 6-digit BSB, or the

			Issuer and *Scheme Name* elements may also be used as described in Option 1.
4	Name + TownName + Country + Id	From the Creditor component: Cdtr/Nm Cdtr/PstlAdr/TwnNm Cdtr/PstlAdr/Ctry Cdtr/Id/OrgId/Othr/Id	If using structured Postal Address, *TownName* + *Country* must be present. This aligns with CBPR+ rules. It is recommended to add Postal Code although it is optional. *Id* is populated with the account number prefixed with the 6-digit BSB, or the *Issuer* and *Scheme Name* elements may also be used as described in Option 2.
5	AnyBIC + Account	From the Creditor component: Cdtr/Id/OrgId/AnyBIC From the Creditor Account component: CdtrAcct/Id/Othr/Id	*AnyBIC* is populated with the 11-digit BIC of the organisation. The *Creditor Account* may be populated with the account number prefixed with the 6-digit BSB, or the *Issuer* and *Scheme Name* elements may also be used as described in Option 1.
6	AnyBIC + Id	From the Creditor component: Cdtr/Id/OrgId/AnyBIC Cdtr/Id/OrgId/Othr/Id	*AnyBIC* is populated with the 11-digit BIC of the organisation. *Id* is populated with the account number prefixed with the 6-digit BSB, or the *Issuer* and *Scheme Name* elements may also be used as described in Option 2.

9.4 Repair BSB:[76]

(a) Today, when payments originate from overseas, the BSB is often missing, and intermediary Framework Participants may insert a repair BSB in order to help processing when making the domestic leg of the payment.[77]

(b) However, the BSB is an optional element in HVCS MX messaging and use of the repair BSB is not mandatory. As a result, intermediary Framework Participants must work towards ceasing the use of repair BSB and recipients should review their back office processing to ensure an empty BSB element will not cause the payment to be rejected.[78]

[76] Amended effective 23/9/24, version 4 r&p 001.24
[77] Amended effective 23/9/24, version 4 r&p 001.24
[78] Amended effective 23/9/24, version 4 r&p 001.24

10. Legal Entity Identifier

The Legal Entity Identifier (LEI) is a 20-character, alpha-numeric code, designed to uniquely identify legally distinct entities that engage in financial transactions. It requires annual verification, carries useful information about company structure, and is the globally recognized ISO 17442 standard. This is an optional element within the HVCS, however, if used, the LEI must be used in combination with account number or BIC or name and address. This practice is consistent with usage prescribed in CBPR+.

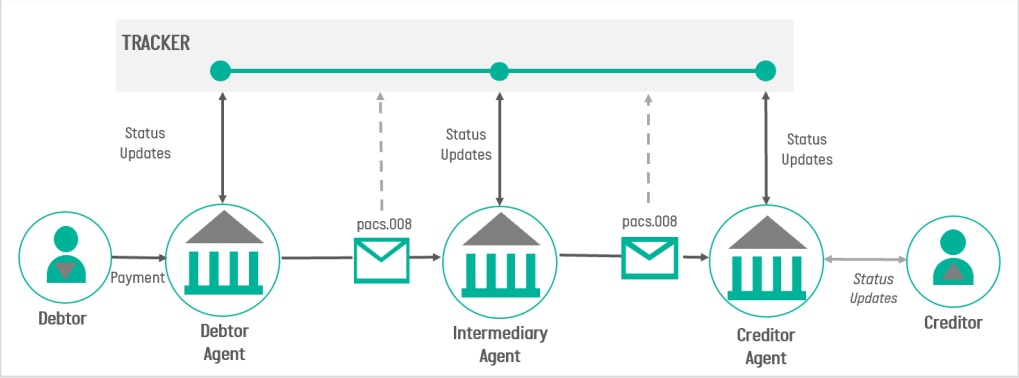
The PMPG have provided extensive guidance in their "Legal Entity Identifier Paper".

11. Payment Confirmation

SWIFT gpi banks must confirm when a payment has been credited to the account of the beneficiary for all pacs.008 and pacs.009 COV messages by sending a gpi Confirmation to the gpi tracker. It is optional for gpi banks to confirm pacs.009 CORE and pacs.004 messages.

SWIFT banks that are not gpi members must confirm all pacs.008 messages with a Universal Confirmation.

These payment confirmations form part of a minimum set of requirements to enhance end-to-end tracking, as shown in the diagram below.



11.1 Service Level Agreement

(a) Outside of the HVCS, payment confirmation is required within two business days following the value date indicated in the pacs.xxx messages for non-gpi members. However, the overall SLA for the HVCS is to clear funds to customer's account on the same day they are received. HVCS Framework Participants must provide confirmation as soon as practically possible after funds have been made available to the customer, and by end-of-day at the latest (accepting that there may be some exceptions such as processing delay caused by payment instructions requiring repair).

12. On Behalf of Payments – Ultimate Debtor and Creditor

For further information regarding 'On Behalf Of' Payments, refer to the 'pacs.008 FI to FI customer credit transfer - Ultimate Debtor and Ultimate Creditor' section of the SWIFT publication "CBPR+ User Handbook".

The next page is Annexure G

ANNEXURE G REFERENCE DATA

The objective of this section is to provide detail on external element code lists and use cases.

1. External Code List[79]

Several elements within the MUGs refer to "External Code Lists". These code lists are maintained by SWIFT (through their quarterly release cycle) and are published for use here. Unless otherwise stated in the MUGs, the HVCS does not restrict use of any of these codes. The below table outlines the code lists that are relevant to the HVCS ISO 20022 message set.

External Code Set Name	head.001 BAH	pacs.008	pacs.009 CORE	pacs.009 COV	pacs.004	camt.029	camt.056
ExternalAccountIdentification1Code	-	✓	✓	✓	✓	-	✓
ExternalCancellationReason1Code	-	-	-	-	-	-	✓
ExternalCashAccountType1Code	-	✓	✓	✓	✓	-	✓
ExternalCashClearingSystem1Code	-	✓	✓	✓	✓	-	-
ExternalCategoryPurpose1Code	-	✓	✓	✓	-	-	-
ExternalClearingSystemIdentification1Code	✓	✓	✓	✓	✓	-	✓
ExternalCreditorAgentInstruction1Code	-	✓	✓	✓	-	-	-
ExternalDiscountAmountType1Code	-	✓	-	✓	-	-	-
ExternalDocumentLineType1Code	-	✓	-	✓	-	-	-
ExternalFinancialInstitutionIdentification1Code	✓	-	-	-	✓	-	✓
ExternalGarnishmentType1Code	-	✓	-	✓	-	-	-
ExternalInvestigationExecutionConfirmation1Code	-	-	-	-	-	✓	-
ExternalLocalInstrument1Code	-	✓	✓	✓	-	-	-
ExternalMandateSetupReason1Code	-	✓	-	-	-	-	-
ExternalOrganisationIdentification1Code	✓	✓	-	✓	✓	-	✓
ExternalPaymentCancellationRejection1Code	-	-	-	-	-	✓	-
ExternalPersonIdentification1Code	✓	✓	-	✓	✓	-	✓
ExternalProxyAccountType1Code	-	✓	✓	✓	✓	-	✓
ExternalPurpose1Code	-	✓	✓	✓	-	-	-
ExternalReturnReason1Code	-	-	-	-	✓	-	-
ExternalServiceLevel1Code	-	✓	✓	✓	-	-	-
ExternalTaxAmountType1Code	-	✓	-	✓	-	-	-

[79] Amended effective 23/9/24, version 4 r&p 001.24

2. Category Purpose – Additional Processing

(a) HVCS Participants are responsible for compliance with any applicable legal, regulatory and reporting obligations, in addition to the HVCS Regulations and Procedures, associated with any HVCS payment and the transmission of payments via the HVCS. From time to time, this may include specific back office processes that may apply to some category purpose codes.

(b) From August 2021, Services Australia ceased using the HVCS to process payments under the Australian Government Code of Operation. As a result, Participants are not required to identify Services Australia payments or put in place any special processing rules for the ISO 20022 CUG.

(c) There are currently no other regulatory requirements in relation to Category Purpose codes, nor are any future requirements planned for domestic usage.

3. Using Payment Message Identifiers

Payment messages can be passed serially between each Participant in the payment chain and contain:

(a) Point-to-point (P2P) elements which are passed between one party to the next, and are not necessarily passed on in subsequent messages (for example, the *Instruction Identification*); and

(b) End-to-end elements (E2E) which are passed unchanged through the entire payment life cycle to all subsequent messages (for example, the *UETR*).

A number of mandatory end-to-end elements contained within *Payment Identification* are used to uniquely identify pacs.008, pacs.009 and pacs.009 COV payment throughout its lifecycle.

The pacs.004 message utilises identifiers at the transaction level as well as from the underlying payment that is being returned within *Original Group Information*.

A summary of payment message identifiers can be found in the table below:

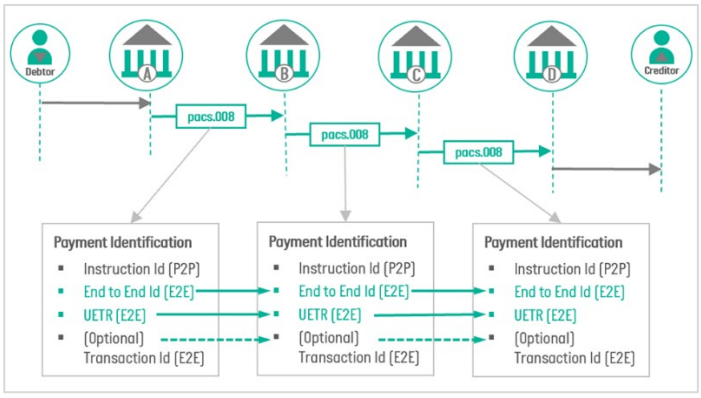
Message	Path	Identifier	Mandatory / Optional	Point to Point (P2P) or End to End (E2E)
pacs.008	GrpHdr/MsgId	*Message Identification*	M	P2P
	AppHdr/MsgDefIdr	*Message Definition Identifier*	M	P2P
	CdtTrfTxInf/PmtId	*Instruction Identification*	M	P2P
		End To End Identification	M	E2E
		Transaction Identification	O	E2E (in the interbank chain)
		UETR	M	E2E
		Clearing System Reference	O	P2P
pacs.009 CORE	GrpHdr/MsgId	*Message Identification*	M	P2P
	AppHdr/MsgDefIdr	*Message Definition Identifier*	M	P2P
	CdtTrfTxInf/PmtId	*Instruction Identification*	M	P2P
		End To End Identification	M	E2E
		Transaction Identification	O	E2E

				(in the interbank chain)
		UETR	M	E2E
		Clearing System Reference	O	P2P
pacs.009 COV	GrpHdr/MsgId	*Message Identification*	M	P2P
	AppHdr/MsgDefIdr	*Message Definition Identifier*	M	P2P
	CdtTrfTxInf/PmtId	*Instruction Identification*	M	P2P
		End To End Identification (from pacs.008)	M	E2E
		Transaction Identification	O	E2E (in the interbank chain)
		UETR (from pacs.008)	M	E2E
		Clearing System Reference	O	E2E
pacs.004	TxInf/RtrId	*Return Identification*	M	P2P
	TxInf/OrgnlGrpInf (optional) [80]	*Original Message Identification*	M	P2P
		Original Message Name Identification	M	P2P
		Original Creation Date Time	O	P2P
	TxInf	*Original Instruction Identification* [81]	O	P2P
		Original End To End Identification	M	E2E
		Original Transaction Identification	O	E2E (in the interbank chain)
		Original UETR	M	E2E
		Original Clearing System Reference	O	P2P

(a) If these elements are not populated in a pacs.004 that originated from cross-border, intermediaries must ascertain them for the domestic leg of the transaction.

(b) It is important to note that this rule is not validated in the MyStandards Readiness Portal and Participants must ensure their messages conform with this requirement.

3.1 Payment Identifiers – pacs.008



[80] The *HVCS_CBPR_OriginalGroupInformationRule* renders *Original Group Information* mandatory in HVCS messaging. In the HVCS, the sub-elements *Original Message Identification* and *Original Message Name Identification* are also mandatory

[81] The HVCS_CBPR_OriginalInstructionIdentificationRule renders *Original Instruction Identification* mandatory in HVCS messaging.

(a) In this example, Bank A is the debtor agent and the first instructing agent in the chain. Bank A must populate *End to End Id* and *UETR*, which are carried forward unchanged by all subsequent banks in the chain. Bank A can also optionally populate *Transaction Identification* and, if populated, it must be carried forward by subsequent banks.

(b) Each bank will populate *Instruction ID* with its own reference. [82]

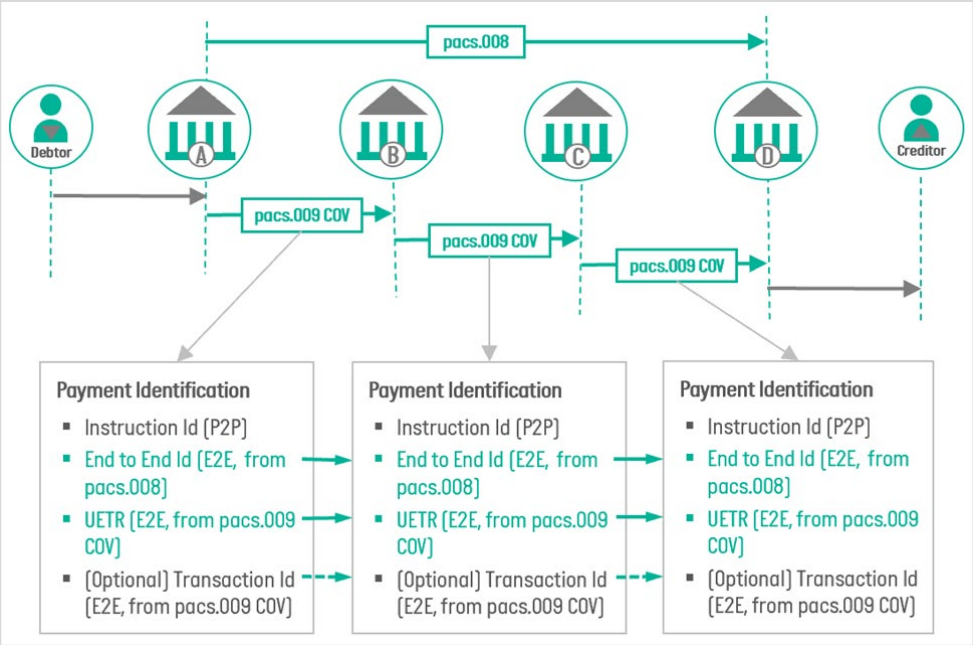
(c) The *Transaction Identification* is assigned by the first instructing agent and is passed on, unchanged, throughout the entire interbank chain. The instructing agent has to make sure that the transaction identification is unique for a pre-agreed period. When a payment is being passed on directly between two banks (i.e., with no Intermediary bank), Bank A could leave *Transaction Identification* blank, as it is an optional reference.

3.2 Payment Identifiers – pacs.009 and pacs.009 COV

(a) The pacs.009 message is used to move funds between financial institutions, either directly between two banks or through a series of banks.

(b) The pacs.009 CORE end-to-end identifiers operate in the same way as the pacs.008 message – identifiers from the first pacs.009 message are carried forward unchanged through each subsequent pacs.009 CORE message in the chain.

(c) The pacs.009 COV is used to settle a pacs.008 customer credit transfer and the two messages together comprise a whole transaction. In order to link the two transactions, the pacs.009 COV carries the *End to End Id* and *UETR* of underlying pacs.008 message.



[82] Amended effective 23/9/24, version 4 r&p 001.24

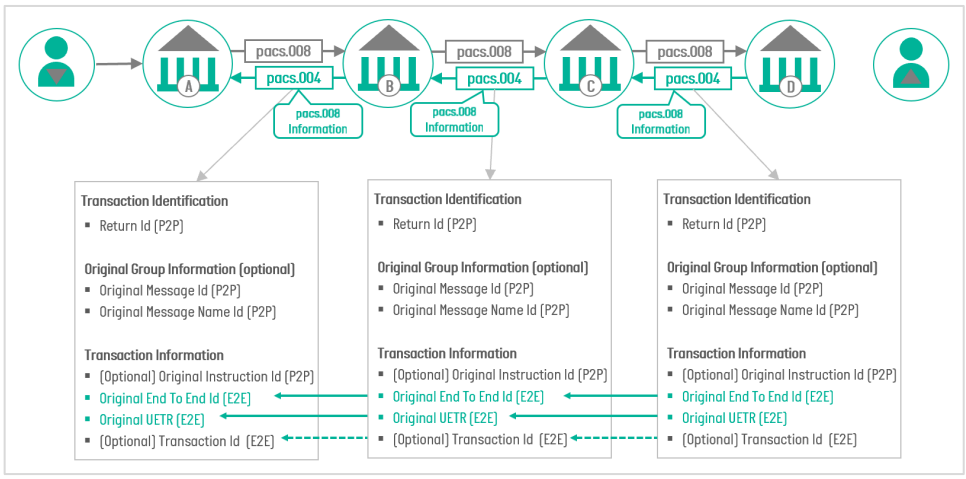
(d) The pacs.009 COV may also carry additional information about the pacs.008 instruction in *Underlying Customer Credit Transfer*. At minimum details about the *Debtor*, *Debtor Agent*, *Creditor Agent* and *Creditor* must be provided.

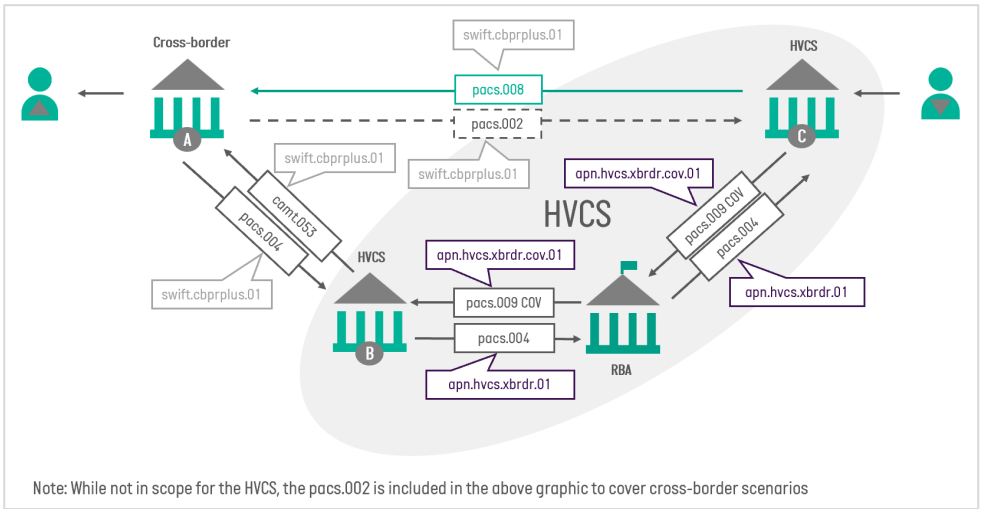
3.3 Payment Identifiers – pacs.004

(a) The pacs.004 is passed from one bank to another bank serially, as shown in the diagram below:

(b) When used to return a pacs.008 or pacs.009 CORE, the pacs.004 Payment Return uses a number of elements to capture identifiers from the underlying payment it is returning. These identifiers are nested within the *Original Group Information* and *Transaction Information*. A number of these elements are mandatory within the HVCS to ensure the pacs.004 conveys sufficient details to the receiving agent to link the return with the payment that was originally sent.

(c) When returning a pacs.009 COV, the pacs.004 follows the path of the pacs.009 COV message as shown below:





(d) Again, the pacs.004 message is sent serially between banks, this time referencing the original pacs.009 COV within *Original Group Information* and *Transaction Information* and with additional key pacs.009 COV elements in *Original Transaction*

Reference. This may include information of the underlying pacs.008 for which cover is provided in the *Underlying Customer Credit Transfer* elements.

4. Population of Mandatory pacs.004 Elements

The following table includes guidance for the population of mandatory pacs.004 elements obtained from the original MX or MT payment, and which allow Participants to link the messages together.

Other mandatory point-to-point elements such as the Return Identification, Instructing Agent and Instructed Agent have not been included in this table.

pacs.004 Element	Original pacs.008, pacs.009 CORE or pacs.09 COV Element	Original MT Element
Original Message Identification <TxInf/OrgnlGrpInf/OrgnlMsgId> (35x)	*Message Identification* <GrpHdr/MsgId> (35x)	Field 20 Sender's Reference (16x)
Original Message Name Identification <TxInf/OrgnlGrpInf/OrgnlMsgNmId> (35x)	*Message Definition Identifier* <AppHdr/MsgDefIdr> (35x) E.g., pacs.008.001.09 or pacs.009.001.09	Block 2 Field 2 SWIFT message Type e.g., 103 or 202 The prefix of *MT* must be added when populating the pacs.004 element with no spaces between the characters, i.e.MT103 or MT202
Original Instruction Identification <TxInf/OrgnlInstrId> (16x)	*Instruction Identification* <CdtTrfTxInf/PmtId/InstrId> (16x)	Field 20 Sender's Reference (16x)
Original End To End Identification <TxInf/OrgnlEndToEndId> (35x)	*End To End Identification* <CdtTrfTxInf/PmtId/EndToEndId> If not provided, insert 'NOT PROVIDED' (35x)	Field 70 Remittance Information code word /ROC/ (Reference of Customer) If not provided, insert 'NOT PROVIDED'
Original UETR <TxInf/OrgnlUETR>	*UETR* <CdtTrfTxInf/PmtId/UETR>	Block 3 – Field 121 UETR (36x)

(36x)	(36x)	
Debtor <TxInf/RtrChain/Dbtr/Pty> This component is populated with Name and Postal Address of the party initiating the return of funds	pacs.008 – *Creditor or Creditor Agent* <FIToFICstmrCdtTrf/CdtTrfTxInf/Cdtr> or <FIToFICstmrCdtTrf/CdtTrfTxInf/CdtrAgt> pacs.009 (CORE/COV) – *Creditor or Creditor Agent* <FICdtTrf/CdtTrfTxInf/Cdtr> or <FICdtTrf/CdtTrfTxInf/CdtrAgt> These components detail the Name and Address	MT103 – Field 59 or 59A Beneficiary (4*35x) MT202 – Field 58a A or D Beneficiary Institution (4*35x) These fields detail the Name, Address and Account Number
Creditor <TxInf/RtrChain/Cdtr/Pty > This component is populated with Name and Postal Address of the party receiving the return of funds	pacs.008 – *Debtor* <FIToFICstmrCdtTrf/CdtTrfTxInf/Dbtr> pacs.009 (CORE/COV) – *Debtor* <FICdtTrf/CdtTrfTxInf/Dbtr> These components detail the Name, Address and Account Number	MT103 – Field 50A, F or K Ordering Customer (4*35x) MT202 – Field 52a A or D Ordering Institution (4*35x) These fields detail the Name, Address and Account Number

The next page is Annexure H

ANNEXURE H TERMINOLOGY

It helps to be familiar with terminology used by SWIFT in ISO20022 messaging to ensure understanding of the common language used.

1. Key Terminology Changes [Deleted]

2. Payment Actors[83]

The following table provides definition of payment actors under ISO 20022:

Type	Definition
Actor	Any participant in the payment chain.
Agent	A participant in the payment chain that executes the movement of funds between, either the bank of the payer, or payee, or an intermediary bank.
Party	A bank client making, initiating or receiving a payment within the chain.
Creditor	Party to which an amount of money is due
Debtor	Party that owes an amount of money to the (ultimate) creditor
Initiating Party	Party that initiates the payment. This might be the payer itself or an agent.
Instructing Agent	Party that instructs the next party in the chain to carry out the (set of) instruction(s).
Instructed Agent	Agent that is instructed by the previous party in the chain to carry out the (set of) instruction(s).
Intermediary Agent	Agent between the debtor's and creditor's agent
Ultimate Creditor	Ultimate party to which an amount of money is due
Ultimate Debtor	Ultimate party that owes an amount of money to the (ultimate) creditor, such as the buyer of services or goods.

The next page is Annexure I

[83] Amended effective 23/9/24, version 4 r&p 001.24

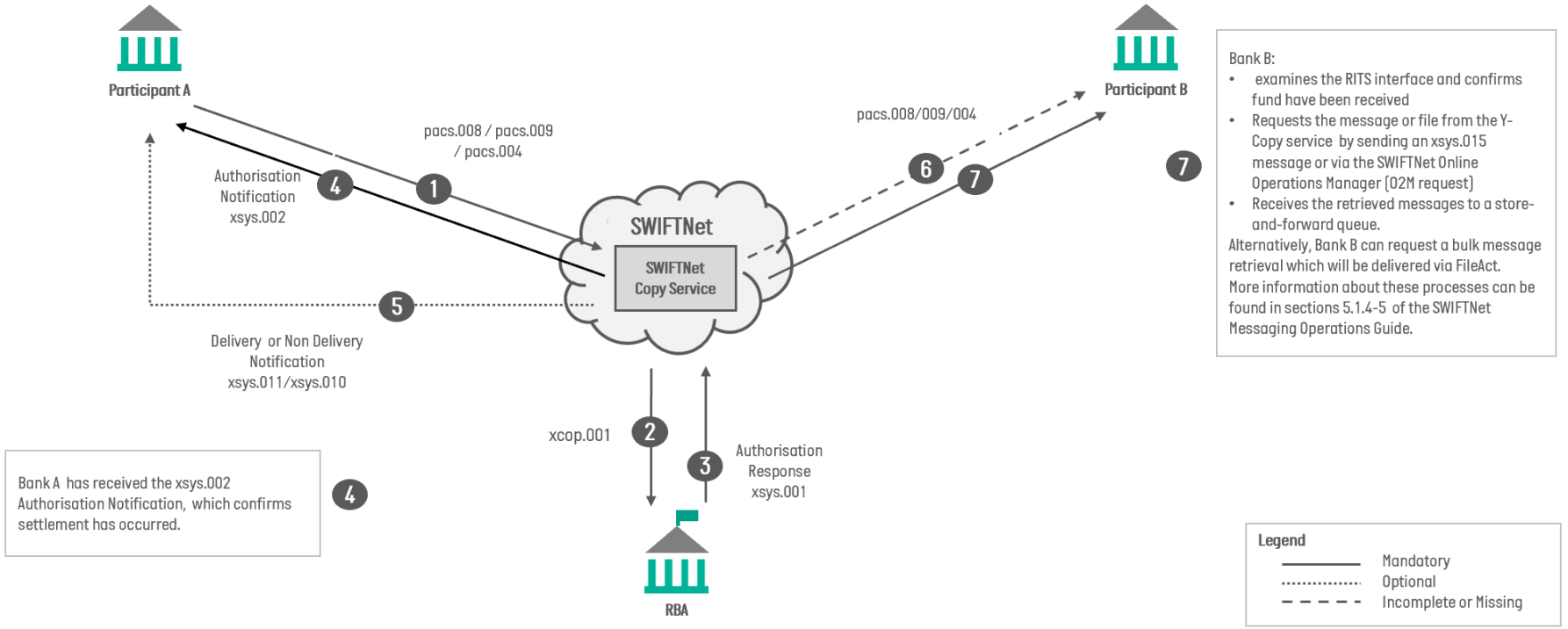
ANNEXURE I BUSINESS USE CASE AND MESSAGE FLOW SCENARIOS

1. Duplicate

The following is an index of scenarios provided in this section:

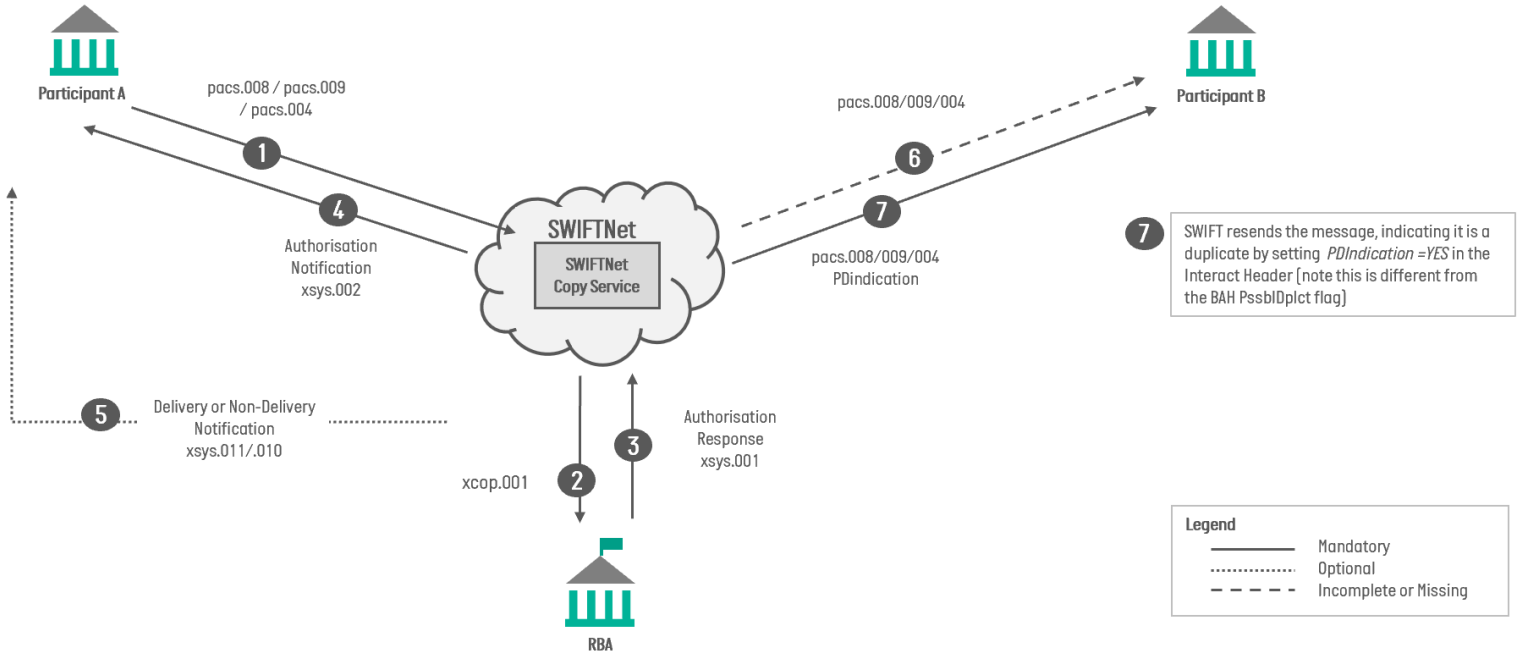
Scenario #	Message Flow/Scenario Description
Scenario 1	Bank A sends a payment, settlement occurs but Bank B can't find the payment
Scenario 2	SWIFT resends a message due to technical connectivity issues
Scenario 3	RITS rejects payment (e.g., outright rejection or due to end-of-day liquidity deficit)
Scenario 4	Bank A is unsure whether a non Y-Copy message was sent successfully
Scenario 5	Bank A sends a non Y-Copy message but Bank B does not receive it (or can't find it)
Scenario 6	Bank A sends a copy of a non Y-Copy message to third party, and then sends a duplicate of the copy
Scenario 7	Bank A is unsure whether a payment has been sent

Scenario 1 - Bank A sends a payment, settlement occurs but Bank B can't find the payment



Guidance:
- Bank A can also examine their RITS interface to confirm funds are no longer in their account, and to view the xcop.001 and xsys.001 messages, but receipt of the xsys.002 message should be sufficient to confirm settlement.
- When retrieving messages from SWIFT, Participants must have robust duplicate checking processes to ensure they do not process messages twice. If both copies of a message are received, one instance should be ignored.

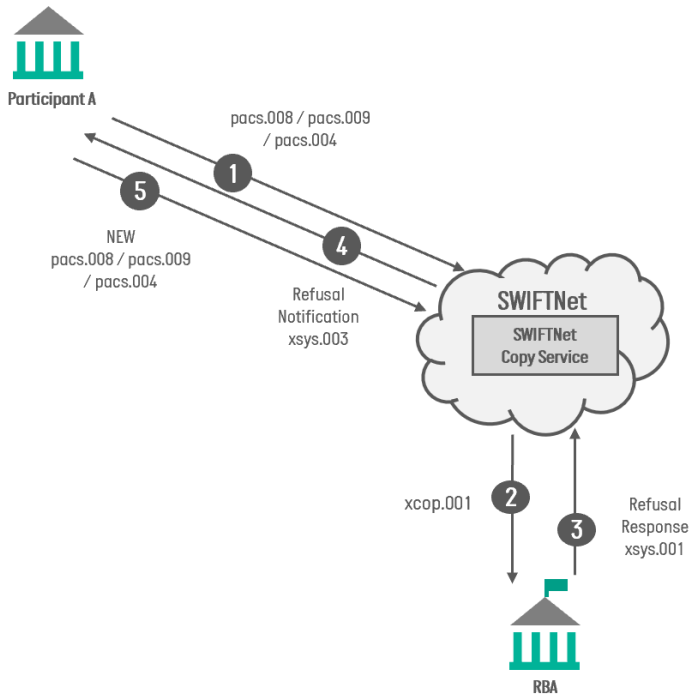
Scenario 2 – SWIFT resends a message due to technical connectivity issues



Guidance:

- Participants must digest the information in the InterAct header in order to identify when PDIndication has been flagged as Y.
- When receiving a message with PDIndication, Participants must put in a process to investigate whether the message is a duplicate to ensure it is not processed twice.
- The receiver should not assume duplicate messages will always arrive after the original message. If both instances of the message are received, one instance should be ignored.

Scenario 3 – RITS rejects payment (e.g. outright rejection or due to end-of-day liquidity deficit)



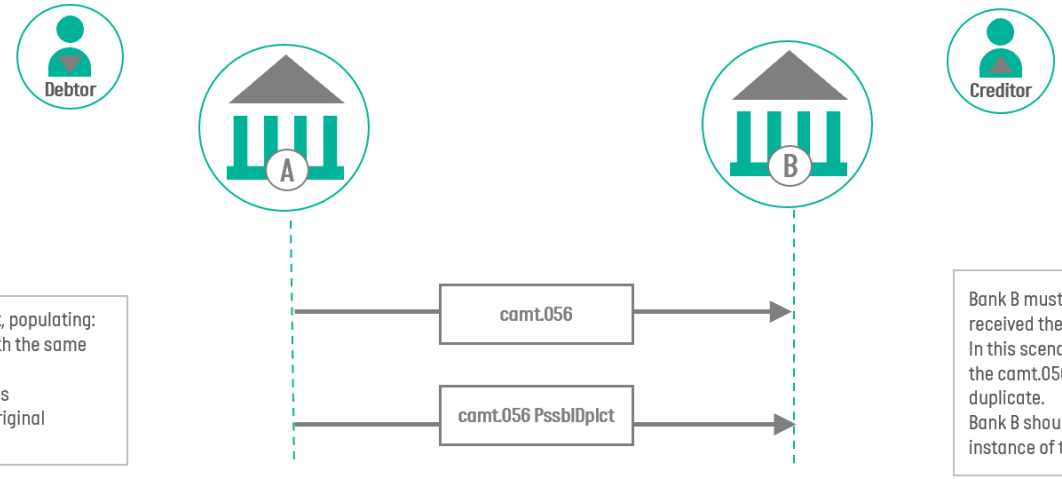
4 Bank A receives an xsys.003 (Refusal Notification) indicating payment has been rejected by RBA. Bank A reviews the refusal reason code and takes action to rectify the issue

5 Bank A must submit a new payment with a difference Instruction (or Return) ID in order to avoid rejection by RITS

Legend
- Mandatory
- Optional
- Incomplete or Missing

Guidance:
- Bank A can also examine their RITS interface to confirm funds are still in their account, and to view the xcop.001 and xsys.001 messages, but receipt of the xsys.003 message should be sufficient to confirm failure of settlement.
- When sending the message again, Participants must ensure the combination of Instruction (or Return) ID and sending BIC is unique within the past 15 calendar days or the payment instruction will be rejected by RITS as a duplicate.

Scenario 4 – Bank A is unsure whether a message was sent successfully

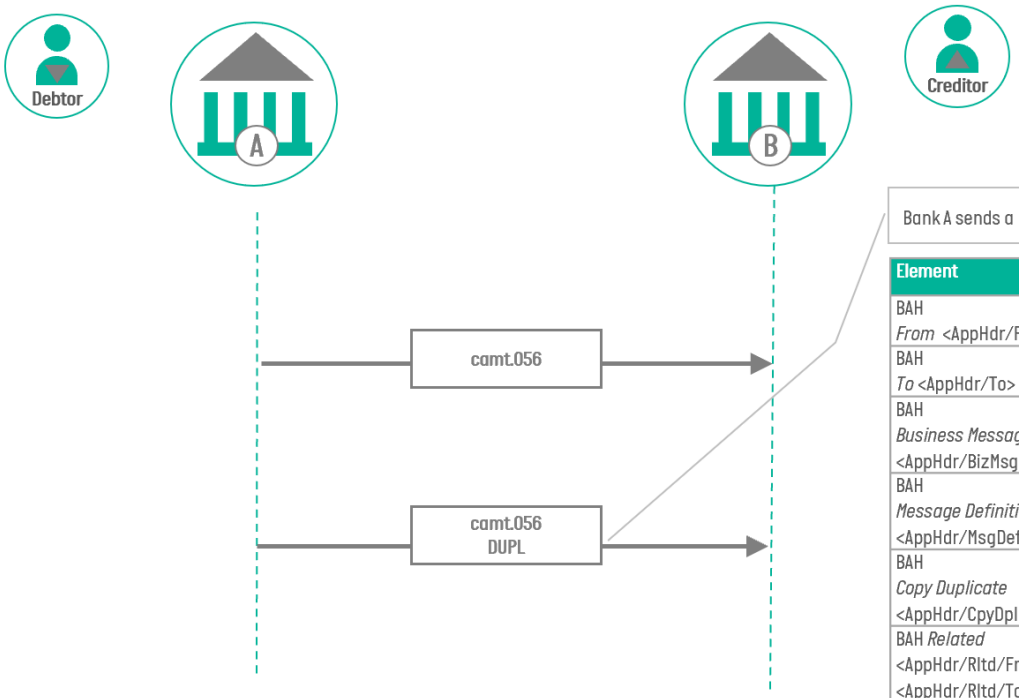


Bank A resends the cancellation request, populating:
- *Case Identification* and *From BIC* with the same details as the original message
- *Possible Duplicate* <PssblDplct> = yes
- *Related* with the BAH details of the original message

Bank B must ascertain whether they have previously received the camt.056 and, if so, ignore one instance. In this scenario, the *Case Identification* element of the camt.056 should be used to help identify the duplicate.
Bank B should respond with a camt.029 to one instance of the message only.

Guidance:
- Resend a message with the BAH *Possible Duplicate* indicator:
  - When reasonable doubt exists about the delivery state of the original message; and
  - When all reasonable efforts have been made to check that the recipient did not receive the response to the message.
- When receiving a message with the BAH *Possible Duplicate* indicator, Participants must put in a process to investigate whether the message is a duplicate to ensure it is not processed twice. The receiver should not assume duplicate messages will always arrive after the original message. If both instances of the message are received, one instance should be ignored.

Scenario 5 – Bank A sends a non Y-Copy message but Bank B does not receive it (or can't find it)



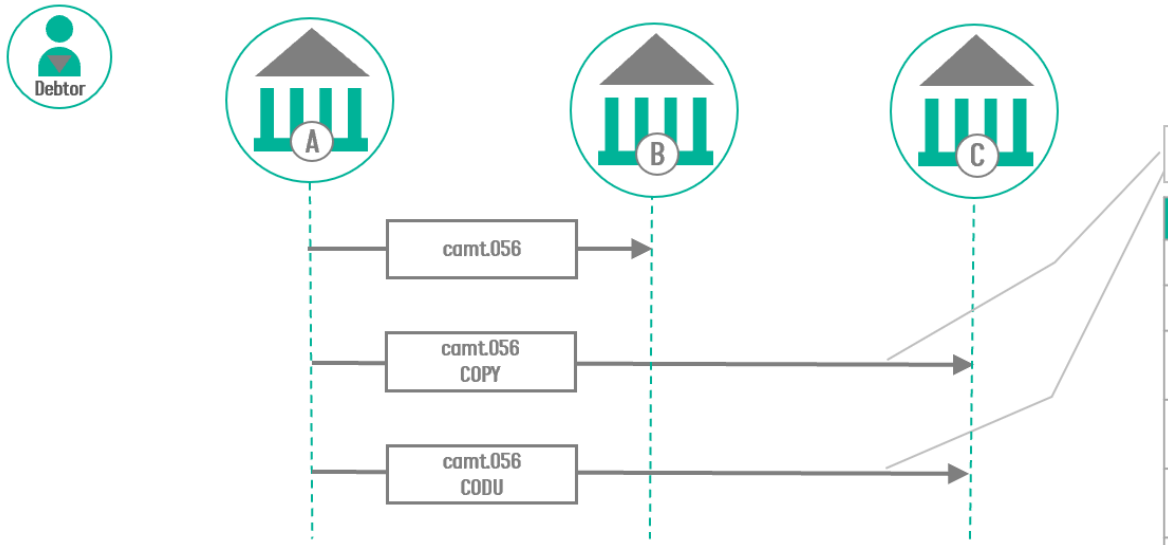
Bank A sends a Duplicate message populating as follows:

Element	Duplicate
BAH *From* <AppHdr/Fr>	Bank A
BAH *To* <AppHdr/To>	Bank B
BAH *Business Message Identifier* <AppHdr/BizMsgId>	Unique identifier of original camt.056
BAH *Message Definition Identifier* <AppHdr/MsgDefIdr>	camt.056.001.xx
BAH *Copy Duplicate* <AppHdr/CpyDplct>	DUPL
BAH *Related* <AppHdr/Rltd/Fr> <AppHdr/Rltd/To> <AppHdr/Rltd/BizMsgId> <AppHdr/Rltd/MsgDefIdr>	Relevant elements from the BAH of the original camt.056

Guidance:

- The *Copy Duplicate* element is used in non Y-Copy messages, as RITS validations will reject duplicate messages sent through the Y-Copy.
- When receiving a message with the duplicate indicator, Participants must put in a process to investigate whether the message is a duplicate to ensure it is not processed twice. The receiver should not assume duplicate messages will always arrive after the original message. If both instances of the message are received, one instance should be ignored.

Scenario 6 – Bank A sends a copy of a non Y-Copy message to third party, and then sends a duplicate of the copy



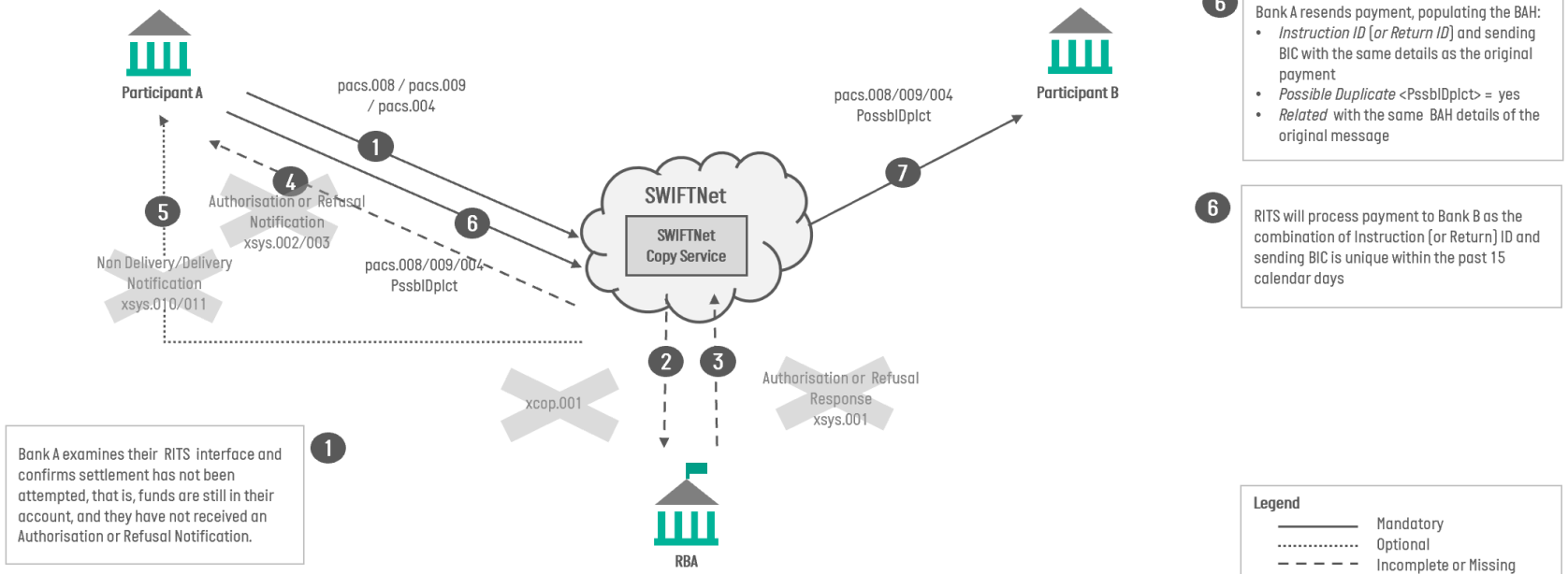
Guidance:

- The *Copy Duplicate* element is used in non Y-Copy messages, as RITS validations will reject duplicate messages sent through the Y-Copy.
- Recipients must ensure their systems are able to recognise COPY or CODU messages and do not process them.
- When the *Copy Duplicate* indicator is set to COPY or CODU, the BAH To BIC does not match the Instructed Agent BIC in the message body and is a unique exception to this rule.

Bank A sends the Copy and CopyDuplicate messages populating as follows:

Element	Copy	Copy Duplicate
BAH *From* <AppHdr/Fr>	Bank A	Bank A
BAH *To* <AppHdr/To>	Bank C	Bank C
BAH *Business Message Identifier* <AppHdr/BizMsgId>	Unique identifier of original camt.056	Unique identifier of original camt.056
BAH *Message Definition Identifier* <AppHdr/MsgDefIdr>	camt.056.001.xx	camt.056.001.xx
BAH *Copy Duplicate* <AppHdr/CpyDplct>	COPY	CODU
BAH *Related* <AppHdr/Rltd/Fr>	Bank A	Bank A
BAH *Related* <AppHdr/Rltd/To>	Bank B	Bank B
Within the message instance: *Instructing Agent* (assigner) <Undrlyg/TxInf/Assgnr>	Bank A	Bank A
Within the message instance: *Instructed Agent* (assignee) <Undrlyg/TxInf/Assgne>	Bank B	Bank B

Scenario 7 - Bank A is unsure whether a payment has been sent



1 Bank A examines their RITS interface and confirms settlement has not been attempted, that is, funds are still in their account, and they have not received an Authorisation or Refusal Notification.

6 Bank A resends payment, populating the BAH:
- *Instruction ID* (*or Return ID*) and sending BIC with the same details as the original payment
- *Possible Duplicate* <PssbIDplct> = yes
- *Related* with the same BAH details of the original message

6 RITS will process payment to Bank B as the combination of Instruction (or Return) ID and sending BIC is unique within the past 15 calendar days

Legend
- Mandatory
- Optional
- Incomplete or Missing

Guidance:
- Although the *Possible Duplicate* element can be used in all MX message types, RITS validations will reject a duplicate message sent through the Y-Copy.
- Resend a message with the BAH *Possible Duplicate* indicator:
  - When reasonable doubt exists about the delivery state of the original message; and
  - When all reasonable efforts have been made to check that the recipient did not receive the response to the message.
- Bank A should populate BAH *Possible Duplicate* as 'yes' in order to distinguish this message from the original, for audit &/or regulatory purposes.
- In the situation where RITS has settled the first message, the second *Possible Duplicate* message will be rejected, and Bank A will receive an xsys.003 Refusal Notification.

2. Exception and Investigation (E&I)

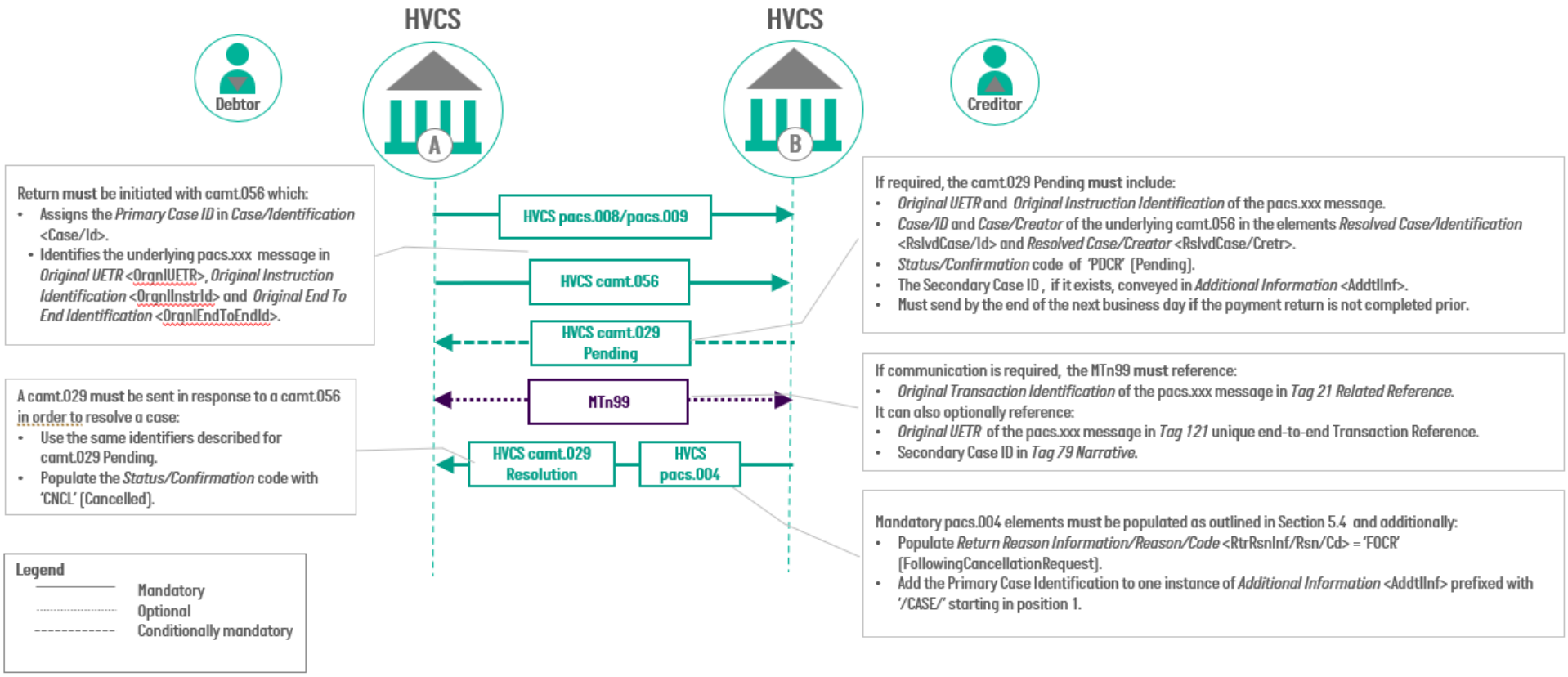
2.1 The following is an index of scenarios provided in this section:[84]

Scenario #	Message Flow/Scenario Description
Scenario 1	HVCS Solicited Payment Return – Using MX *E&I* messaging
Scenario 2	Solicited Payment Return – Payment Originating from HVCS – Using MX *E&I* messaging
Scenario 3	Solicited Payment Return – Payment Originating from CBPR+ – Using MX *E&I* messaging
Scenario 4	Solicited Payment Return – Payment Originating from CBPR+ – Using MX *E&I* messaging – Bypassing the Intermediary Participant
Scenario 5	Unsolicited Payment Return – Payment Originating from HVCS – Multiple Partial Payments
Scenario 6	HVCS Solicited Payment Return - Using MX Messaging - Multiple Partial Payments
Scenario 7	Solicited Payment Return – Payment Originating from HVCS - Using MX *E&I* messaging - Multiple Partial Payments
Scenario 8	Return of a Payment Return
Scenario 9	Cross-Border General Investigation

[84] Amended effective 23/9/24, version 4 r&p 001.24

Scenario 1 – HVCS Solicited Payment Return – Using MX E&I Messaging

Scenario: Participant A sends a payment to Participant B but then requests it to be returned.

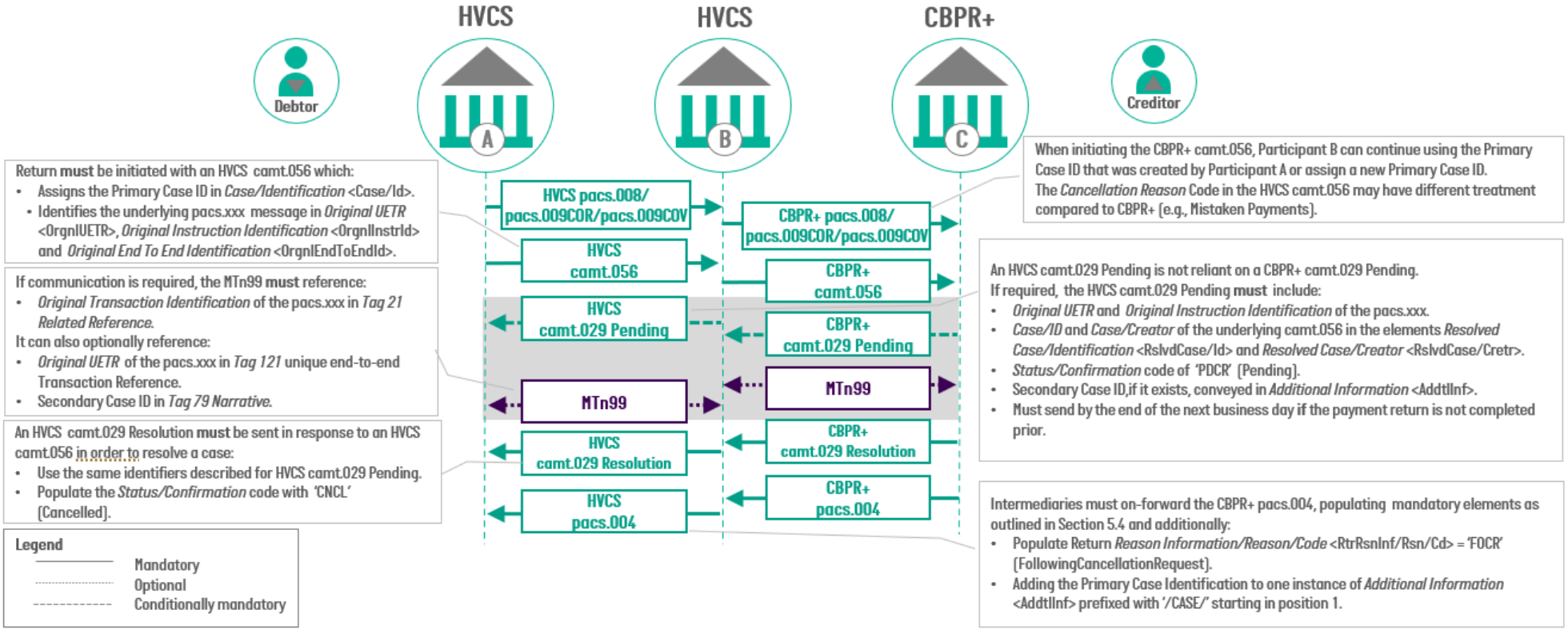


Scenario 2 – Solicited Payment Return – Payment Originating from HVCS – Using MX E&I Messaging

Scenario: Participant A is acting as the domestic HVCS Participant.

General Guidance:

- Intermediary Participant B must determine how to populate the HVCS version of each message when sending through the domestic CUG to Participant A .
- The HVCS investigation between Participants A & B is a separate case to the CBPR+ investigation between Participant B & Bank C and follow different market practice guidance and SLAs. Intermediary Participant B must reconcile the CBPR+ investigation and the HVCS investigation separately.
- The messages and message types used for the HVCS investigation and the CBPR+ investigation will differ, and one-to-one messaging equivalence is not required (i.e. the HVCS camt.029 message is not the same or equivalent to the CBPR+ camt.029 message).

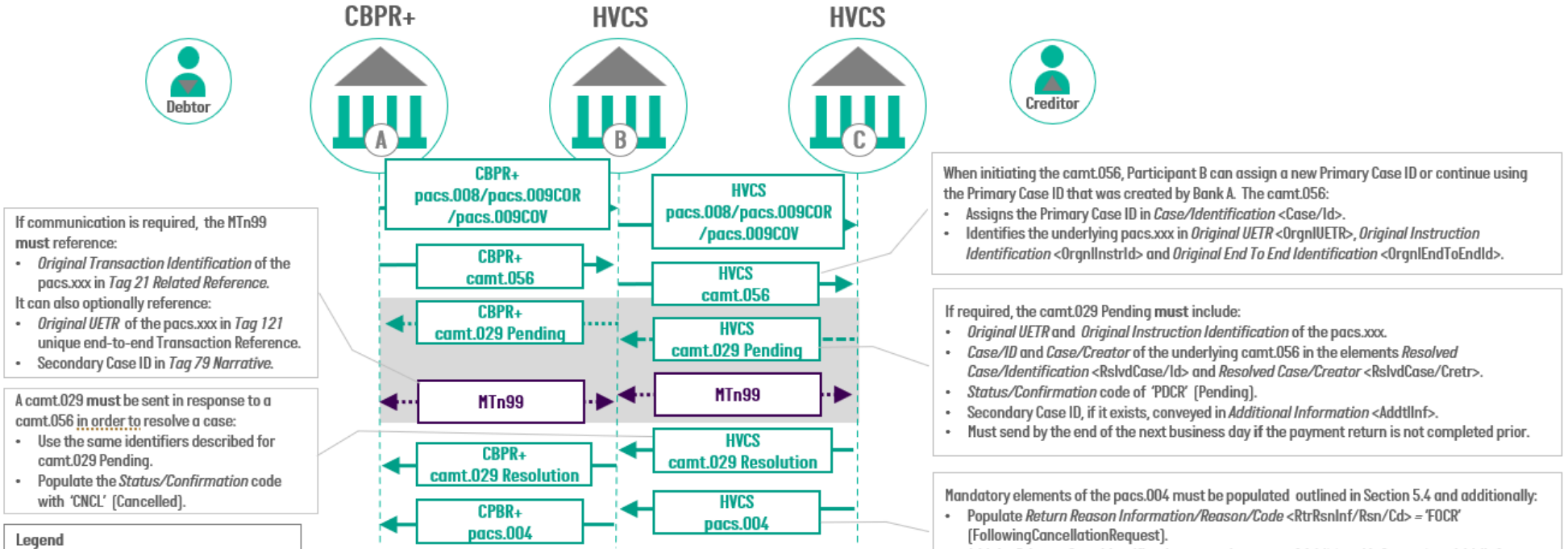


Scenario 3 – Solicited Payment Return – Payment Originating from CBPR+ – Using MX E&I Messaging

Scenario: Bank A is a CBPR+ bank.

Guidance:

- Intermediary Participant B must determine how to populate the HVCS version of each message when sending through the domestic CUG to Participant C.
- The CBPR+ investigation between Bank A & Participant B is a separate case to the HVCS investigation between Participants B & C and follow different market practice guidance and SLAs. Intermediary Participant B must reconcile the CBPR+ investigation and the HVCS investigation.
- The messages and message types used for the HVCS investigation and the CBPR+ investigation will differ, and one-to-one messaging equivalence is not required [i.e. the HVCS camt.029 message is not the same or equivalent to the CBPR+ camt.029 message].



If communication is required, the MTn99 **must** reference:

- *Original Transaction Identification* of the pacs.xxx in *Tag 21 Related Reference.*

It can also optionally reference:

- *Original UETR* of the pacs.xxx in *Tag 121* unique end-to-end Transaction Reference.
- Secondary Case ID in *Tag 79 Narrative.*

A camt.029 **must** be sent in response to a camt.056 in order to resolve a case:

- Use the same identifiers described for camt.029 Pending.
- Populate the *Status/Confirmation* code with 'CNCL' (Cancelled).

Legend

- Mandatory
- Optional
- Conditionally mandatory

When initiating the camt.056, Participant B can assign a new Primary Case ID or continue using the Primary Case ID that was created by Bank A. The camt.056:

- Assigns the Primary Case ID in *Case/Identification* <Case/Id>.
- Identifies the underlying pacs.xxx in *Original UETR* <OrgnlUETR>, *Original Instruction Identification* <OrgnlInstrId> and *Original End To End Identification* <OrgnlEndToEndId>.

If required, the camt.029 Pending **must** include:

- *Original UETR* and *Original Instruction Identification* of the pacs.xxx.
- *Case/ID* and *Case/Creator* of the underlying camt.056 in the elements *Resolved Case/Identification* <RslvdCase/Id> and *Resolved Case/Creator* <RslvdCase/Cretr>.
- *Status/Confirmation* code of 'PDCR' (Pending).
- Secondary Case ID, if it exists, conveyed in *Additional Information* <AddtlInf>.
- Must send by the end of the next business day if the payment return is not completed prior.

Mandatory elements of the pacs.004 must be populated outlined in Section 5.4 and additionally:

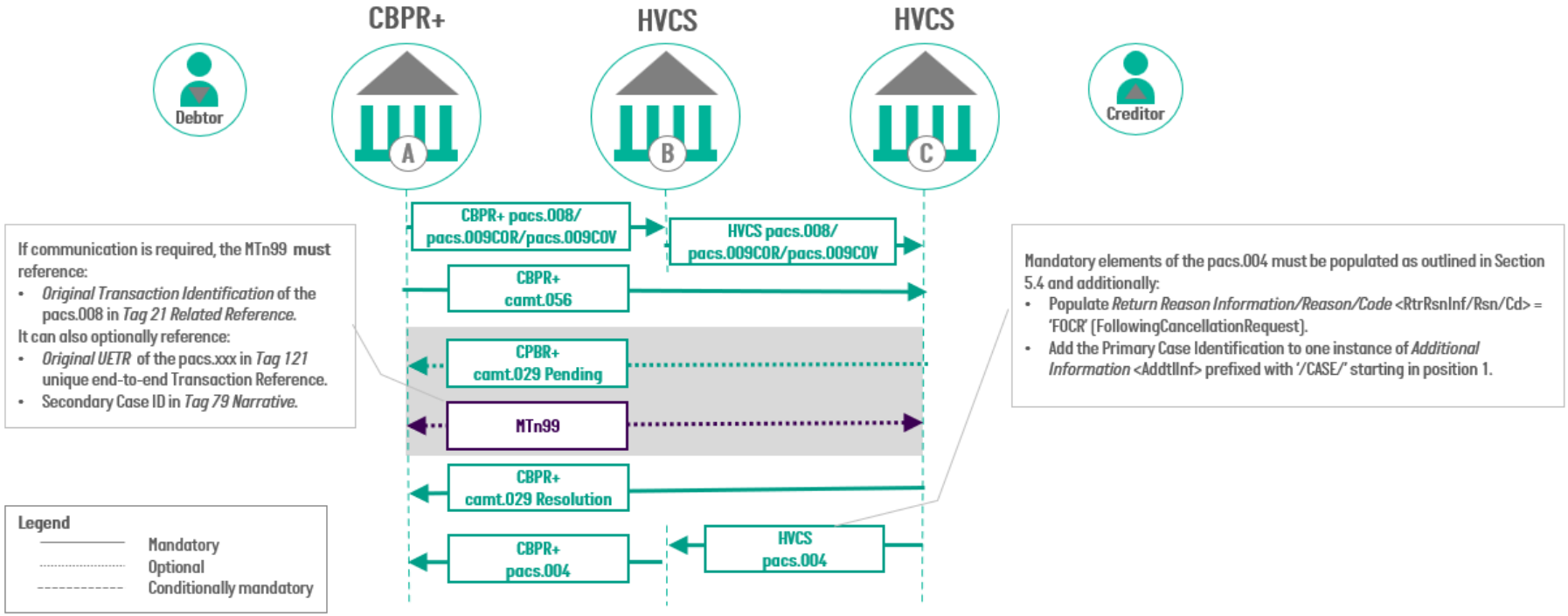
- Populate *Return Reason Information/Reason/Code* <RtrRsnInf/Rsn/Cd> = 'FOCR' (FollowingCancellationRequest).
- Add the Primary Case Identification to one instance of *Additional Information* <AddtlInf> prefixed with '/CASE/' starting in position 1.

Scenario 4 – Solicited Payment Return – Payment Originating from CBPR+ – Using MX E&I Messaging – Bypassing the Intermediary Participant

Scenario: CBPR+ Bank A sends a payment to HVCS Participant C via HVCS Intermediary Participant B. However, as Participant C is also a CBPR+ Bank, Bank A sends the return request (camt.056) directly to Participant C, bypassing Participant B.

Guidance:

- If the investigation is to be continued through CBPR+, CBPR+ rules should be followed.
- As Participant B is not be aware of the messaging being conducted directly between Participant A and C, it should simply onforward the return payment unchanged.



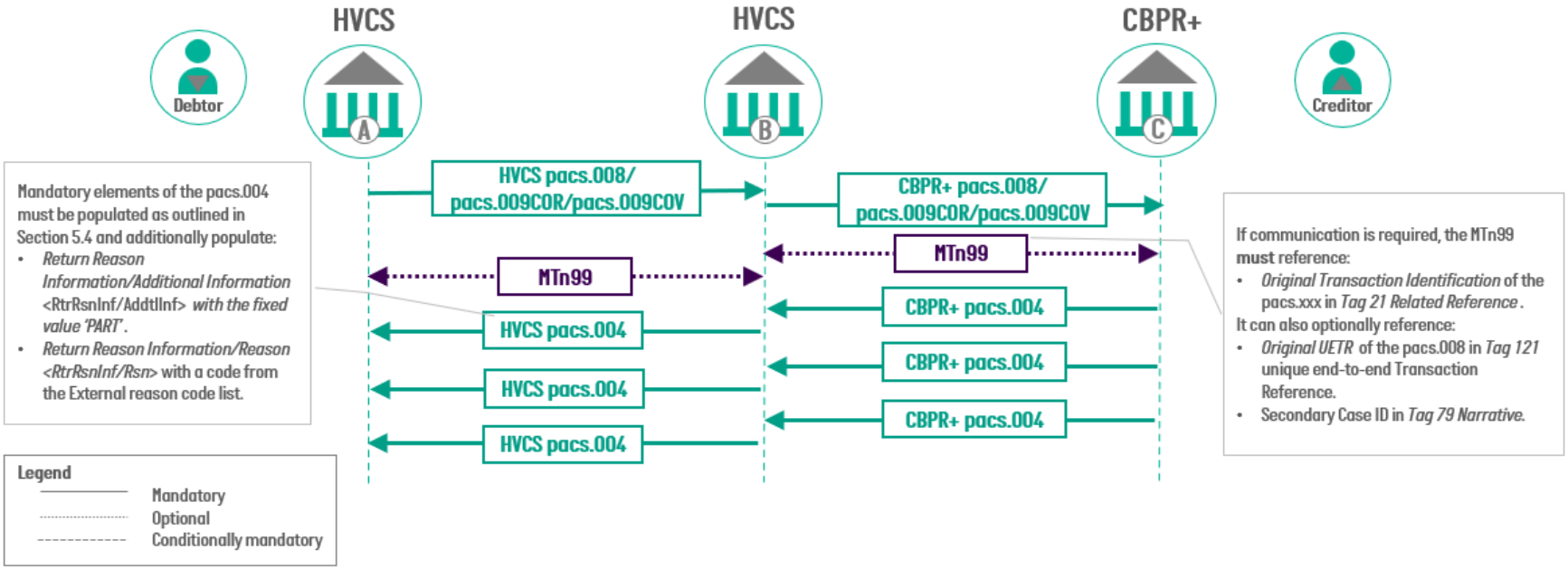
Scenario 5 – Unsolicited Payment Return – Payment Originating from HVCS – Multiple Partial Payments

Scenario:

- HVCS Participant A sends a payment to CBPR+ Bank C, via intermediary Participant B.
- Bank C returns the payment to Participant B in instalments, which forwards them to Participant A.

Guidance:

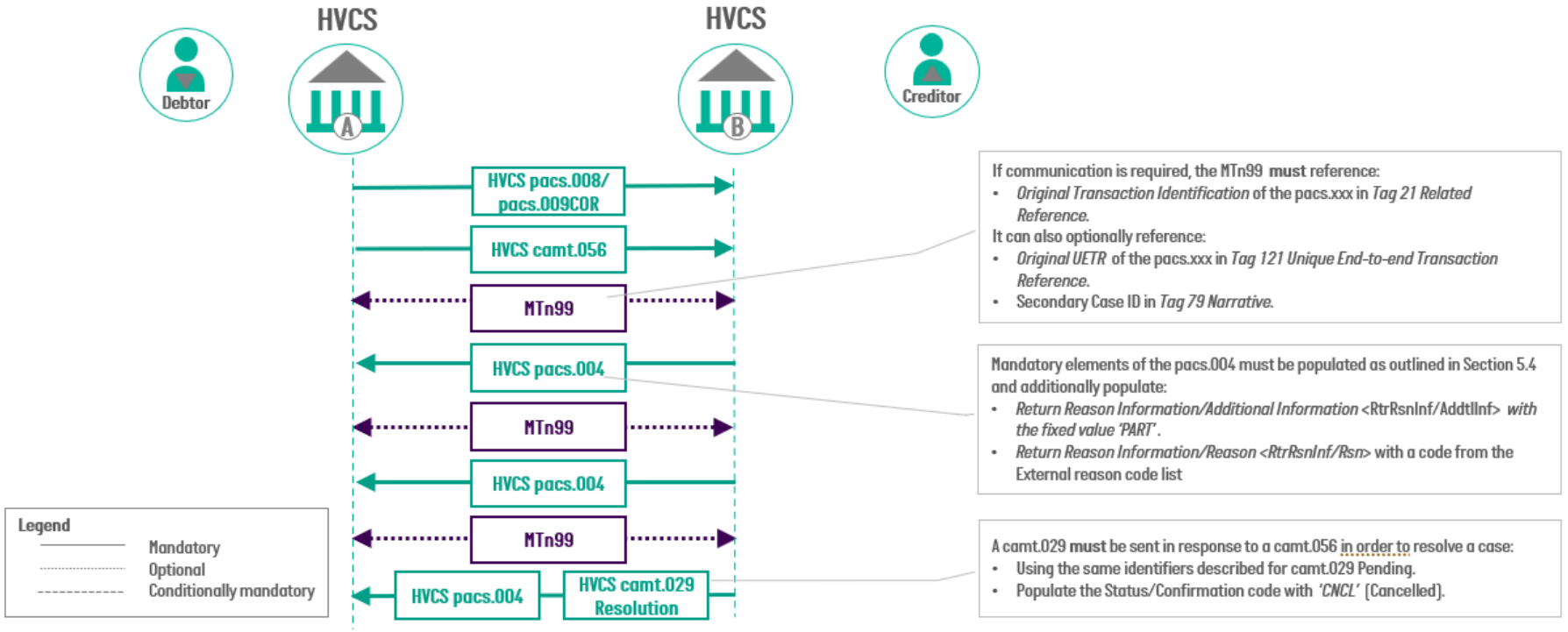
- Intermediary Participant B must pass on the pacs.004 messages as received and add point-to-point references.
- If Bank C sends any other messages, Participant B should forward them to Participant A.
- A domestic unsolicited payment return must be made in a single amount which can be different to the original amount. However, multiple partial payment returns may be received from CBPR+.



Scenario 6 – HVCS Solicited Payment Return – Using MX Messaging – Multiple Partial Payments

Scenario: Participant A sends a pacs.xxx to Participant B and then requests a payment return using a camt.056. Participant B returns the payment in multiple instalments.

Guidance: A domestic solicited payment return may be made in multiple instalments, but an unsolicited payment return must be made in a single amount.



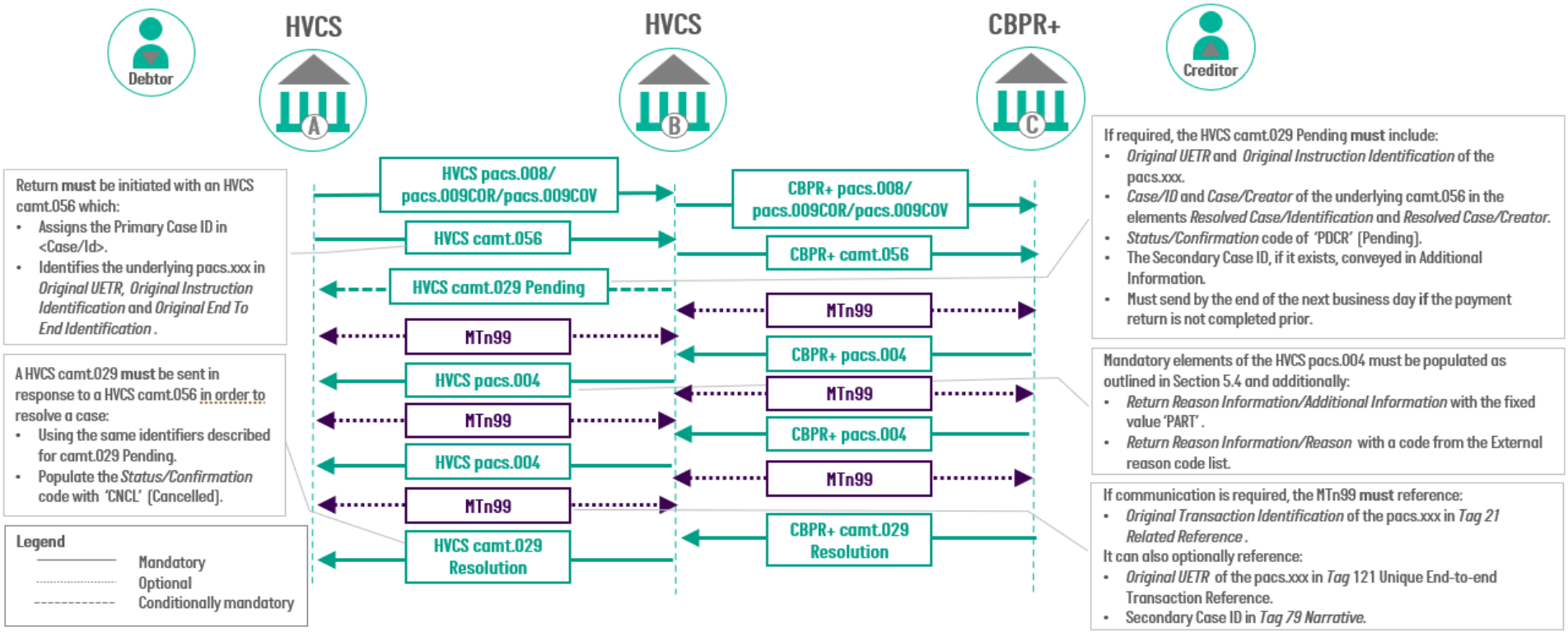
Scenario 7 – Solicited Payment Return – Payment Originating from HVCS – Using MX E&I Messaging – Multiple Partial Payments

Scenario:

- HVCS Participant A sends a pacs.xxx to CBPR+ Bank C via HVCS Intermediary Participant B.
- Participant A requests for the funds to be returned by sending an HVCS camt.056 to Participant B, Participant B sends a CBPR+ camt.056 to CBPR+ Bank C.
- Bank C returns the payment to Participant B via multiple partial payments using pacs.004 and Participant B forwards each partial payment and associated messaging to Participant A.

Guidance:

- Intermediary Participant B must pass on the pacs.004 messages as received and adding point-to-point references.
- If Bank C sends any other messages, Participant B should forward them to Participant A.
- The HVCS investigation between Participants A & B is a separate case to the CBPR+ investigation between Participant B & Bank C and must be reconciled separately by Participant B.



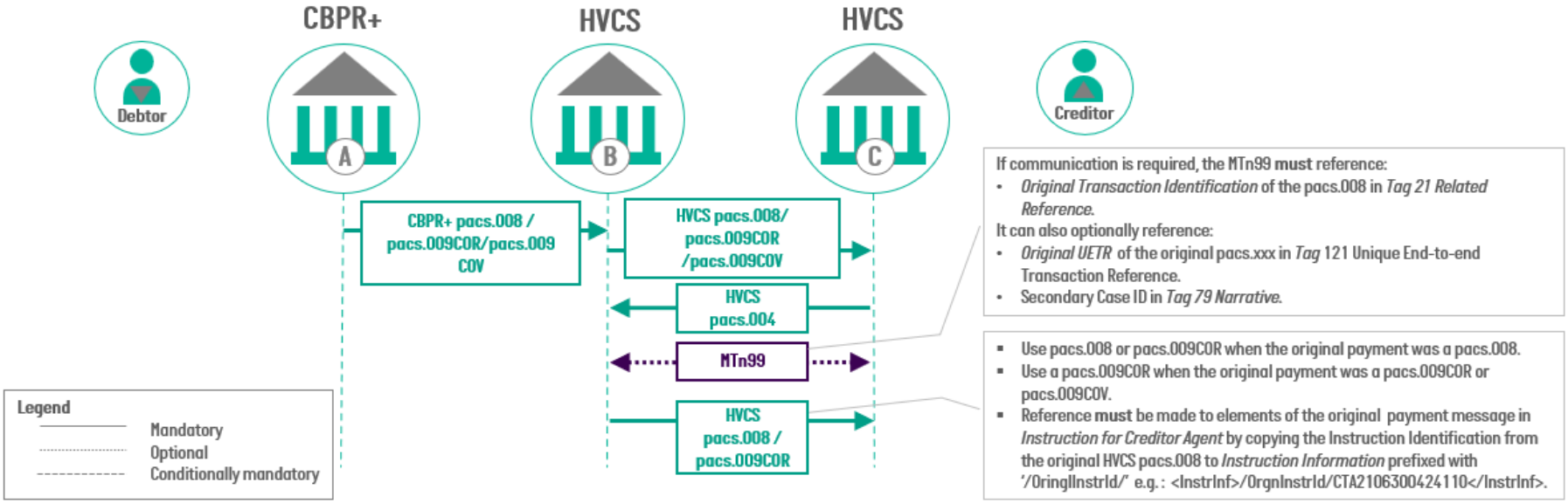
Scenario 8 – Return of a Payment Return

Scenario:

- CBPR+ Bank A sends a pacs.xxx to Participant C via intermediary Participant B. Participant C mistakenly refuses funds and returns the payment to Participant B via a pacs.004.
- In subsequent communication with Participant B, Participant C realises its error and the payment is returned using pacs.008 or pacs.009 COR.

Guidance:

- Participants cannot use the pacs.004 message to complete a Payment Return of a Payment Return.
- When completing a payment return of a payment return, ensure that the original Debtor and Creditor elements are captured.
- In the converse scenario, a return of a payment return may be initiated by CBPR+ Bank A as a pacs.004. In this case, there is no requirement for intermediary Participant B to convert it to a pacs.008 for the HVCS leg of the transaction. Participant B should simply pass on the pacs.004 as received.

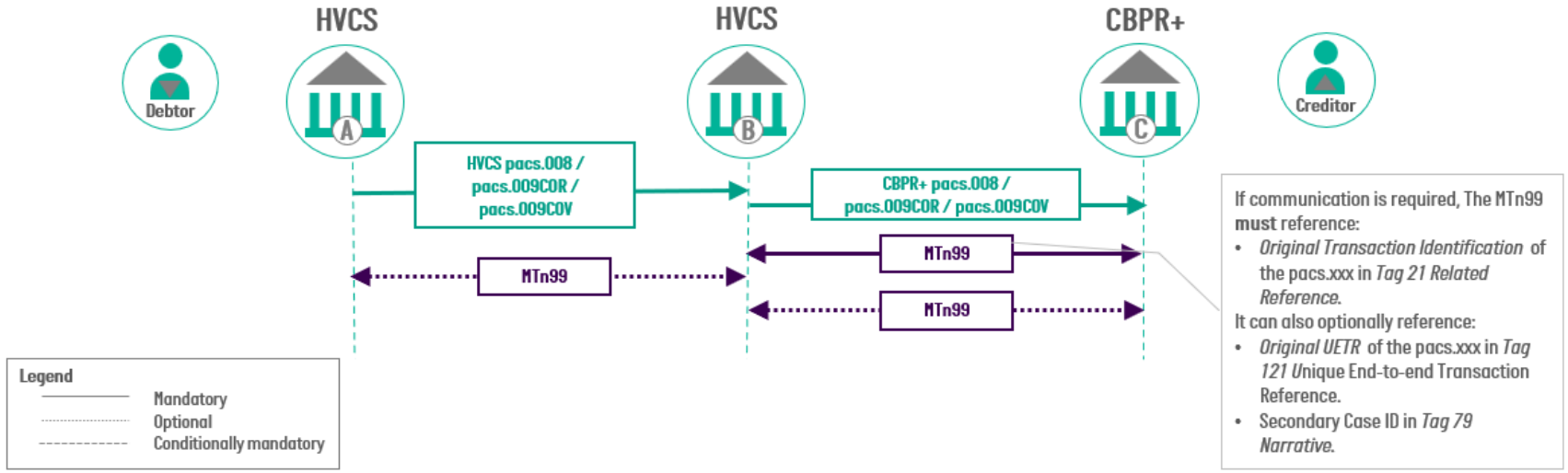


Scenario 9 – General Investigation involving a CBPR+ Bank

Scenario:

- Participant A sends a pacs.xxx message to CBPR+ Bank C via intermediary Participant B.
- Bank C is unable to apply funds and sends an MTn99 free format message Participant B, which then sends an MTn99 to Participant A.
- Participant A responds with corrected account number details, enabling Bank C to processes the payment.

Guidance: Communication between HVCS Participants A & B is separate to any offshore communication between Participant B & Bank C and one-to-one messaging equivalence is not required.



The next page is Annexure J

ANNEXURE J CONTINGENCY INSTRUCTIONS FOR THE HIGH VALUE CLEARING SYSTEM

1. Introduction

These Contingency Instructions provide instructions and guidance for High Value Clearing System (HVCS) Framework Participants (Participants) to ensure the continuity of orderly clearing and settlement in the event that either:

(a) a Participant experiences a Disabling Event that prevents it from sending HVCS payments in the normal way; or

(b) the Reserve Bank of Australia (RBA) experiences a Disabling Event that prevents the Reserve Bank Information and Transfer System (RITS) from settling HVCS payments in the normal way.

Participants must comply with the instructions set out in this document.

1.1 Relationship with other documents

Document	Relationship / Purpose	Owner
HVCS Contingency Industry Test Strategy	The high-level strategy for testing HVCS contingency arrangements.	AusPayNet
HVCS Contingency Industry Test Plan	The detailed test plan for industry contingency test exercises. A test plan is produced for each annual test.	AusPayNet
HVCS Exchange Summary Form	A summary document substantially in the format prescribed by the RBA, and available on the Company's extranet. Used by a Framework Participant to submit its net bilateral obligations with each of its counterparties to the RBA for net settlement the next day.	RBA
HVCS Bilateral Clearing Form	A document in a format prescribed by the Company used by an Affected Participant to send HVCS payments to another Framework Participant.	AusPayNet
RITS Member Contingency Procedures (MCP)	High-level procedures to be followed by RITS Members if a contingency disrupts the efficient operation of RITS or the Fast Settlement Service (FSS) over an extended period.	RBA
AusPayNet Member Incident Plan (MIP)	Framework for industry coordination during an operational incident affecting the HVCS.	AusPayNet
AusPayNet Crisis Communication Plan (CCP)	Framework for industry and media communication during a major disruption to any of the payments systems or infrastructure that fall under the remit of the Company.	AusPayNet

2. Scope

These Contingency Instructions provide instructions and guidance for Framework Participants in the event of an extended RITS Outage or an extended Participant Outage. The Contingency Instructions are intended to set a baseline of operational requirements and expectations among Participants to ensure the continuity of HVCS payments during a HVCS Fallback Period or a Participant Fallback Period.

2.1 Applicable Scenarios

2.1.1 RITS Outage

This is a period during which the RBA is experiencing a Disabling Event that prevents RITS from effecting settlement of HVCS payments in the normal way. The scenario would be such that the RBA has ruled out the possibility to resolve the Disabling Event in time to complete settlement of HVCS payments in the normal way on that day. Where this occurs, the Company, after consultation with the RBA, can declare a HVCS Fallback Period during which the HVCS Fallback Solution will be used to enable same-day clearing to occur, with settlement deferred to the next business day. The HVCS Fallback Solution comprises:

Fallback Clearing	Same-day clearing through the SWIFT PDS in T-Copy Mode.
Fallback Settlement	Deferred (next-day) multilateral net settlement using data submitted to the RBA from Participants in HVCS Exchange Summary Form spreadsheets.

In the case of a RITS outage, the copy mode of both the MT CUG and ISO 20022 CUG will switch to T-Copy. Participants must continue to operate in both CUGs in accordance with the Procedures relevant to each CUG.[85]

2.1.2 Participant Outage

This is a period during which a Participant is experiencing a Disabling Event that prevents that Participant from sending HVCS payments in the normal way. The scenario would be such that the Affected Participant, in consultation with the Company and the RBA, is not confident that the Disabling Event can be resolved in time to send any payments deemed urgent by the Affected Participant before the RITS cut-off times. Where this occurs, the Company can declare a Participant Fallback Period during which the Participant Fallback Solution can be used to enable same-day clearing of the Affected Participants outbound HVCS payments to continue, with settlement of the net bilateral obligations occurring on the same day via RITS Cash Transfers. The Participant Fallback Solution comprises:

Fallback Clearing	Outbound payments: Clearing information sent from the Affected Participant to each Receiver using the HVCS Bilateral Clearing Form. Note that inbound payments will continue to be sent to the Affected Participant through the SWIFT PDS in the normal way.
Fallback Settlement	Outbound payments: Deferred (same-day) bilateral net settlement using RITS Cash Transfers. Note that the settlement of inbound payments received by RITS through the SWIFT PDS feeder will be effected in the normal way (RTGS).

[85] Amended effective 23/9/24, version 4 r&p 001.24

2.1.3 Out of Scope

Arrangements for the following Contingency scenarios are outside the scope of these Contingency Instructions:

(a) Disabling Events occurring at the Participant, RITS or CSI level that can be resolved on the same day, within the checkpoint times outlined in the RITS Outage Runsheet and Participant Outage Runsheet contained in these Contingency Instructions.

(b) Contingency arrangements for a Disabling Event at the SWIFT Network level.

(c) Contingency arrangements for HVCS payments to or from CLS Bank. During a RITS Outage, Participants must not send payments to CLS Bank using the HVCS Fallback Solution. A CLS AUD holiday could be declared in such circumstances, in accordance with the CLS Bank's own contingency procedures.

(d) Whilst it is permissible, it is unlikely that a Participant experiencing a Disabling Event will choose to use these contingency arrangements to send the domestic leg of an inbound cross-border payment.

2.2 Document Structure

The Contingency Instructions for each of the two outage scenarios are divided into the following sections:

Section	Description
Runsheets	Checkpoint times and sequence of events for declaring a Fallback Period and using the Fallback Solution
Instructions	*Operational Readiness*: Pre-requisites and preparation for a Fallback Period. *Participation:* Who participates during a Fallback Period. *Entering Fallback*: Declaring a Fallback Period and invoking the Fallback Solution. *During Fallback*: Using the Fallback Solution. *Exiting Fallback*: Decision and processes to exit a Fallback Period. *Operational Capacity*: Payment volumes when using the Fallback Solution. *Applying Funds*: Applying funds received through the Fallback Solution to Customer accounts.

2.3 Classification of Instructions

These Contingency instructions can be applied under Part 9 of these Procedures which is designed to enable orderly operation of the HVCS during a Contingency. In accordance with clause 9.2 of these Procedures, Participants have a responsibility to each other, and to the system as a whole, to cooperate in resolving any processing difficulties. To the extent that such co-operation does not adversely affect its own processing environment, a Participant should provide such co-operation.

There are three classifications of instructions:

Rating	Definition
Must	Participants are required to implement all 'Must' items. These *requirements*: • define a minimum level of functionality in order for a Fallback Solution to be viable and meet its objectives; • enable Participants to meet their clearing obligations and minimise disruption to Customers.
Should	Participants are expected to implement 'Should' items. These *expectations:* • provide instructions and guidance on aspects of the Fallback Solution that may vary based on the specifics of a Participants systems or operations.
Could	Participants are encouraged to consider 'Could' items but are not required to implement them. These *considerations*: • provide indications of recommended best practice.

2.4 Classification of Framework Participants

These Contingency Instructions classify Participants into Back-up Tiers in accordance with clause 7.4 of these Procedures.

1. RITS Outage Runsheet

This runsheet outlines the checkpoint times and sequence of events for a HVCS Fallback Period. It is based on the following assumptions:

(a) The priority is recovering RITS in order to resume normal operations. As such, a decision to declare a HVCS Fallback Period is unlikely to be taken ahead of the checkpoint times outlined. However, where a recovery of RITS has been ruled out ahead of the checkpoint times, then ensuring ongoing clearing of HVCS payments becomes a priority and a HVCS Fallback Period may be declared earlier. Once active, T-Copy mode will remain in place for the duration of the PDS Operating Day.

(b) HVCS Fallback operations for the day, up to and including the submission of HVCS Exchange Summary Forms to the RBA (Step 6), should be complete by 21:00.

(c) To achieve this, the decision to declare a HVCS Fallback Period should be taken by 16:00. Where it is necessary to delay this decision, the 21:00 completion time may also be delayed and the time available to Participants for clearing payments using the HVCS Fallback Solution (Step 4) may be reduced.

(d) If a Disabling Event occurs after 15:00, the assumption is that a HVCS Fallback Period would not normally be required; however the RBA would assess the conditions and potential systemic impact on the day of the event.

(e) In all cases, a decision to declare a HVCS Fallback Period will not be taken within one hour of a Disabling Event occurring in order to allow for sufficient investigation by the RBA. Participants should begin preparing for a potential HVCS Fallback Period when a Disabling Event occurs, but will be given a minimum of 30 minutes from when the HVCS Fallback Period is declared to the implementation of the HVCS Fallback Solution.

Step / Checkpoint		Time	Description	Who
Before	RITS Disabling Event occurs and incident coordination begins.	Before 15:00	A Disabling Event prevents RITS from effecting settlement in the normal way. An incident is raised and managed in accordance with the AusPayNet Member Incident Plan and if applicable, the Crisis Communication Plan. The RBA works to resolve the issue and recover RITS. Participants are aware of the potential for a HVCS Fallback Period and begin to prepare.	RBA, AusPayNet and Participants

	Decision taken to invoke HVCS Fallback Period.	By 16:00	The RBA determines RITS cannot be recovered in time to complete settlement and the Company declare a HVCS Fallback Period.	RBA and AusPayNet
Checkpoint	**HVCS Fallback decision point.**	**16:00**	**Decision to declare HVCS Fallback Period to be made by this time.**	
Step 1	SWIFT instructed to change SWIFTNet Copy Service mode.	15 min	A Business Officer instructs SWIFT via the SWIFT Secure Channel. The Business Officer will request that SWIFT close the service and effect the change no earlier than 30 minutes from the time that the HVCS Fallback Period was declared to Participants.	AusPayNet or RBA
Step 2	SWIFT undertake SWIFTNet Copy Service mode change.	45 min	SWIFT enact the service mode change. SWIFT require a maximum of 45 minutes to do this (i.e. from the point of being instructed to the point that the service reopens in T-Copy mode).	SWIFT
Checkpoint	**T-Copy start time.**	**17:00**	**PDS to be operating in T-Copy mode by this time.**	
Step 3	RBA confirms change of mode to Participants.	5 min	The RBA notify Participants upon receiving confirmation from SWIFT that the mode has changed.	RBA
Step 4	Clearing continues in T-Copy.	2 hrs	Participants exchange HVCS payments. This could include clearing up to a full day's volume of payments, including any additional steps Participants must perform when operating in T-Copy. The RBA will notify Participants of the approaching T-Copy Cut-off Time 30 minutes before the Cut-off Time.	Participants
Step / Checkpoint		**Time**	**Description**	**Who**
Checkpoint	**T-Copy Cut-off time.**	**19:00**	**No further T-Copy clearing to occur after this time.**	
Step 5	SWIFT instructed to change SWIFTNet Copy Service mode.	5 min	A Business Officer instructs SWIFT via the SWIFT Secure Channel to change the SWIFTNet Copy Service from T-Copy to Y-Copy mode.	AusPayNet or RBA
Step 6	Participants compile and submit provisional HVCS Exchange Summary Forms to RBA.	2 hrs	Participants record the net bilateral obligations arising from the payments exchanged in Step 4 in the HVCS Exchange Summary Form. Each Participant sends one HVCS Exchange Summary Form to the RBA. The RBA confirms receipt of these via encrypted email. Resolution of discrepancies and failures to match is performed in Step 8.	Participants

Step 7	RBA produces and sends Provisional HVCS Exchange Figures Advice to Participants.	1 hr	The RBA generate a Provisional HVCS Exchange Figures Advice for each Participant based on the HVCS Exchange Summary Forms submitted in Step 6. Any mismatching net bilateral positions between Participants will be displayed in this advice. The advices will be sent to Participants via encrypted email. Participants have until the commencement of the Morning Settlement Session the next day to reconcile any discrepancies with other Participants and submit a revised version of their HVCS Exchange Summary Form to the RBA (see Step 12).	RBA
Step 8	Overrun buffer.	2 hrs	Buffer if Steps 1 to 7 overrun. Participants can use this time to resolve mismatching net bilateral positions advised by the RBA in Step 7.	-

Step / Checkpoint		Time	Description	Who
Checkpoint	**Midnight.**	**00:00**	**Hard cut-off time. Step 7 must be complete by this time.**	
Step 9	RITS recovery continues.	6.5 hrs	Where necessary, the RBA continue work to recover RITS ready for the overnight processing required before the next day.	RBA
Step 10	RITS reports and overnight processing occurs.		RBA proceed with normal report production and overnight processing required to prepare RITS for the next day.	
Step 11	RITS connection to SWIFT Feeder restored.		Once RITS is recovered and the system date has rolled forward, the SWIFT Feeder connection is restored. The backlog of settlement requests held in the CSI from T-Copy clearing the previous day will enter RITS and be rejected due to the back-dated value date. Senders can use the RITS UI to view the record of rejected T-Copy settlement requests (see Step 12).	
Checkpoint	**RITS available.**	**06:30**	**RITS to be available by this time to prepare contingency batch.**	
Step 12	Participants perform optional reconciliation of HVCS Exchange Summary Forms to RITS.	30 min	Using the RITS UI, Participants can export a record of payments sent in T-Copy the previous day (Step 4) and rejected by RITS (Step 11). Participants can also obtain a record of payments settled or rejected by RITS prior to the Disabling Event using statements produced in Step 10, or the RITS UI.	Participants

			Participants can elect to use these RITS records to reconcile the net obligations in their Exchange Summary Forms which may help to resolve a failure to match discrepancy identified in Step 7. Where required, Participants can submit a revised HVCS Exchange Summary Form to the RBA at any time between Step 8 and Step 12 (inclusive).	

Step / Checkpoint		Time	Description	Who
Checkpoint	**HVCS Exchange Summary Form discrepancies rectified.**	**07:00**	**RBA applies Failure To Match (FTM) rules to all remaining discrepancies.**	
Step 13	RBA produces and sends Final Exchange Figures Advice & Net Clearing System Obligations Advice to Participants.	30 min	The RBA apply FTM rules in accordance with clause 9.25 of these Procedures to any remaining discrepancies in Participant's HVCS Exchange Summary Form and sends a Final HVCS Exchange Figures Advice to Participants via encrypted email. This will include a Net Clearing System Obligations Advice that shows a Participant's multilateral net position in the contingency batch, including clearing interest	RBA
Checkpoint	**RITS Morning Settlement Session starts.**	**07:30**	**RBA enters the contingency batch in RITS at the commencement of the Morning Settlement Session (MSS).**	
Step 14	Participants pre-fund ESAs.	25 min	Where required, Participants pre-fund their ESA in preparation for settlement of the contingency batch.	Participants
Step 15	Contingency batch entered in RITS and settlement testing begins.	5 min	Batch obligations could settle immediately if all Participants in the batch have sufficient ESA funds.	RBA
Step 16	Contingency batch settlement testing period.	30 min	Participants with a shortfall of ESA funds must finalise funding within this 30 minute window. Settlement testing for the contingency batch times out after 30 minutes.	Participants
Checkpoint	**Contingency batch settled.**	**08:45**	**If the contingency batch has not settled by the end of this period the RBA may extend the MSS as necessary until the batch is settled.**	
After	9.00am batch settlement occurs.	30 min	Only processing associated with the 9.00am batch can be undertaken during this session. The contingency batch cannot settle in this session.	RBA

Checkpoint	**RITS Daily Settlement Session starts.**	**09:15**	**RITS Daily Settlement Session will not begin until the previous day's HVCS obligations have settled.**	
After	Normal operations resume.	-	HVCS payments dispatched on the current day clear in Y-Copy mode.	-

2. Participant Outage Runsheet

This runsheet outlines the checkpoint times and sequence of events for a Participant Fallback Period. It is based on the following assumptions:

(a) The priority is recovering the Affected Participant's Disabling Event in order to resume normal operations. As such, a decision to declare a Participant Fallback Period is unlikely to be taken ahead of the checkpoint times outlined. However, if the Affected Participant has urgent payments to send and cannot estimate their recovery time; or is able to rule out a recovery ahead of the checkpoint times, then minimising the delay to payments becomes a priority and a Participant Fallback Period could be declared earlier.

(b) Where the Affected Participant has not recovered by 15:00, a Participant Fallback Period could be declared, during which time the Participant Fallback Solution can be used to send payments from the Affected Participant to Receivers. Payments to the Affected Participant must continue to go through the SWIFT PDS and will be queued in the Affected Participant's SWIFT systems until their inward processing is restored. These payments will continue to be tested and settled in RITS as per the normal operation of the SWIFT PDS Feeder.

(c) The Participant Fallback Period checkpoints are linked to RITS session times and rules. This allows Receivers to effectively manage their end of day liquidity operations and ensure they have sufficient operational staff available.

(d) Outgoing payments from the Affected Participant to Receivers should be complete by the end of the RITS Settlement Close Session at 17:15. The checkpoint times and instructions regarding the frequency of bilateral clearing and settlement should enable the Affected Participant to send and settle at least one batch of payments per Receiver. Where the Affected Participant is Evening Agreed and wishes to send payments to another Evening Agreed Participant after the Settlement Close Session, the Affected Participant must obtain prior agreement from the Receiver. These payments must be complete by the Evening Settlement Cut-off.

(e) Where the volume of payments the Affected Participant intends to send a Receiver exceeds the instructions on payment volumes, the Affected Participant must obtain prior agreement from the Receiver.

(f) If the Affected Participant's Disabling Event occurs after 14:00, the Company, in consultation with the RBA, would normally expect that a Participant Fallback Period would not be required, but would consider the value of outstanding payments in its assessment.

Step / Checkpoint		Time	Description	Who
Before	Disabling Event occurs and incident coordination begins.	Before 14:00	A Disabling Event occurs that prevents the Affected Participant from sending HVCS payments in the normal way. An incident is raised and managed according to the AusPayNet Member Incident Plan. The Affected Participant works to resolve the issue. All Participants are aware of the potential for a Participant Fallback Period and begin to prepare. During this period, the Affected Participant actively manages their ESA balance and where necessary, recycles liquidity via RITS Cash Transfers. Other Participants must be able to pause outbound payments to the Affected Participant if requested to do so by the Affected Participant.	RBA, AusPayNet and Participants
	Decision taken to declare a Participant Fallback Period.	By 15:00	If the Affected Participant has not recovered by this time, the Company, in consultation with the RBA and the Affected Participant, declare a Participant Fallback Period.	AusPayNet, RBA and Affected Participant

Checkpoint	**Participant Fallback decision point.**	**15:00**	**Decision to declare a Participant Fallback to be made by this time.**	
Step 1	Affected Participant sends payments using the HVCS Bilateral Clearing Form and enters corresponding RITS CT.	60 min	The Affected Participant produces and sends a HVCS Bilateral Clearing Form to Receivers; and enters the corresponding bilateral settlement obligations to RITS via Cash Transfer.	Affected Participant
Step 2	Receivers accept the HVCS Bilateral Clearing Form and enter corresponding RITS CT.	30 min	Receivers review the HVCS Bilateral Clearing Form received from the Affected Participant and enter the corresponding bilateral settlement obligation to RITS via Cash Transfer.	Other Participants
Checkpoint	**RITS Daily Settlement Session ends.**	**16:30**	**Cut-off for sending payments.**	
Step 3	RITS CT matched and bilateral obligations settle.	-	Settlement occurs when the Cash Transfers input by the Affected Participant and Receiver are matched in RITS, subject to the Affected Participant having sufficient ESA funds.	-
Step 4	Receivers post payments to Customer accounts.	45 min	The Receiver should aim to apply funds received from the Affected Participant to Customer accounts before the RITS Settlement Close Session ends. Where this is not possible, the Receiver could inform the Affected Participant of the expected completion time.	Other Participants

Checkpoint	**RITS Settlement Close Session ends.**	**17:15**	**Cut-off for settlement of payments.**	
-	Overrun buffer.	45 min to 3 hr 15	The Affected Participant can send additional payments during this period if they and the Receiver are both Evening Agreed and where the Receiver agrees to accept the payments.	Affected Participant
Checkpoint	**RITS Evening Settlement cut-off.**	**18:30 19:30 20:30**	**Cut-off for settlement of Evening Agreed Participant payments.**	

3. RITS Outage Instructions

3.1 Operational Readiness

The following instructions cover items that Participants are expected to have in place in preparation for a HVCS Fallback Period.

3.1.1 Operational Readiness

Participants **must** be operationally ready to continue to participate in the HVCS if a HVCS Fallback Period is declared. This includes:

1. being familiar with these Procedures and the Contingency Instructions;
2. being capable of making the internal system and operational changes required to send and receive payments during the HVCS Fallback Period;
3. participating in contingency test exercises coordinated by the Company; and
4. ensuring staff are available and contactable at all times during the HVCS Fallback Period and during planned contingency test exercises.

Participants **must** attest to their adherence with these requirements as part of the completion of the Yearly Audit Compliance Certificate (Annexure B).

3.1.2 Projected ESA Balance

Participants **must** have reliable and preferably system-based methods for tracking their bilateral net settlement obligations and projected ESA balance during a HVCS Fallback Period.

Note: Depending on the nature of the Disabling Event, it may not be possible for Participants to obtain the most recent record of their ESA balance from RITS. As such, Participants must be ready to use the last-known ESA balance according to their own internal records or obtained from RITS prior to the Disabling Event.

3.1.3 Non-Current Day Payments

Participants **must** have reliable and preferably system-based methods for preventing future-dated and back-dated payments from being sent in SWIFT T-Copy[86] and for identifying future-dated and back-dated payments received in error.

86 SWIFT does not perform date validations on payment messages sent to the SWIFTNet Copy Service and as such, these messages will be delivered straight to the Receiver when T-Copy mode is in operation.

3.1.4 Processing Rules

Participants **should** establish system rules required to smoothly handle differences between SWIFT T-Copy messages compared to SWIFT Y-Copy. Requirements will depend on the configuration of Participants internal systems. For example:

(a) Senders will not receive xsys.002 or xsys.003 responses from RITS for payments sent under T-Copy. Participants that rely on these messages should have a system-based method to account for this in their downstream processing.

(b) The Third Party To Sender Information/ Third Party To Receiver Information elements are not populated;

(c) The Copy State element within Request Descriptor of the Copy in the InterAct header is populated with T-Copy Fallback instead of Active; and

(d) In the SWIFTNet interface, only one signature will be received.

3.2 Participation

The following instructions describe the extent to which Participants are expected to participate in the HVCS when a HVCS Fallback Period has been declared.

3.2.1 Extent of Participation

When a HVCS Fallback Period has been declared and the SWIFT PDS is operating in T-Copy Mode:

1. All Participants must continue to accept payments received from another Participant. Instructions for applying incoming funds to Customer accounts are set out in Section 6.7.

2. Tier 1 Participants must continue to send payments in accordance with the operational capacity instructions in Section 6.6.

3. Tier 2 Participants should continue to send payments in accordance with the operational capacity instructions in Section 6.6 but can, where it determines in advance that it will not send payments, elect to opt-out, in accordance with 6.2.2.

4. All Participants must manage their forecast liquidity position during the HVCS Fallback Period, taking account of the net bilateral obligations due for settlement in the contingency batch the next day.

3.2.2 Participation Opt-Out

Tier 2 Participants that do not intend to continue sending payments during a HVCS Fallback Period **must** have pre-agreed this arrangement with the Company. Where there are extenuating circumstances in which the Tier 2 Participant needs to send payments during a HVCS Fallback Period, the Tier 2 Participant **must** notify and obtain prior agreement from the Receiver.

Note: list of pre-agreed Tier 2 Participants will be available from the AusPayNet extranet site such that during a HVCS Fallback Period, it is clear that other Participants should not expect to receive payments from those on the list.

3.2.3 SWFT Connectivity

Participants **must** remain connected to the SWIFT PDS during the HVCS Fallback Period. That is, a Participant must not disable its connection to the SWIFT network via physical or logical means or deliberately undertake any action that would result in them being unable to send or receive payments via the SWIFT PDS.

3.3 Entering HVCS Fallback

The key checkpoint times for declaring and entering a HVCS Fallback Period are set out in the RITS Outage Runsheet. In summary, where a Disabling Event prevents RITS from settling HVCS payments the priority is recovering RITS in order to resume normal system operations. As such, a decision to declare a HVCS Fallback Period is unlikely to be taken ahead of the checkpoint times outlined. However, if the RBA rule out a recovery of RITS ahead of the checkpoint times, then minimising the delay to payments becomes the priority and a HVCS Fallback Period could be declared earlier. If a Disabling Event occurs after 15:00, the RBA would not normally expect to declare a HVCS Fallback Period, but would assess the conditions and potential systemic impact on the day of the event. In all cases, a decision to declare a HVCS Fallback Period will not be taken within one hour of a Disabling Event occurring in order to allow for sufficient system investigation by the RBA.

The following instructions apply once a HVCS Fallback Period has been declared.

3.3.1 Participant Preparation Time

Participants **should** begin preparing for a potential HVCS Fallback Period when a Disabling Event occurs, but will be given a minimum lead time of 30 minutes from the decision to declare a HVCS Fallback Period to its implementation. The Company or the RBA will instruct SWIFT to close the SWIFTNet Copy Service and effect the change to T-Copy no earlier than 30 minutes from the time that the HVCS Fallback Period was declared to Participants.

Transition to SWIFT T-Copy

The Company or the RBA inform SWIFT of the incident by phone call and foreshadow the impending action to change the SWIFTNet Copy Service from Y-Copy to T-Copy mode. The instruction is formally lodged with SWIFT using the SWIFT Secure Channel.[87]

Upon instruction, SWIFT commence the procedure to switch the SWIFTNet Copy Service mode. Switching modes takes up to 45 minutes. The transition between Y and T-Copy occurs smoothly with no halt to processing of messages.

87 Information available at https://www.swift.com/myswift/secure-channel

3.3.2 Notifying Participants

The RBA will notify Participants upon receiving confirmation from SWIFT that the SWIFTNet Copy Service mode has been changed. Service notifications will be sent to RITS Operational Contacts via email and SMS. [88]

3.3.3 Confirmation of ESA Balance

If possible , the RBA will provide Participants with confirmation of their last known ESA balance prior to entering the HVCS Fallback Period. This may not be possible if the Disabling Event prevents the RBA from accessing this information, in which case, Participants **must** use their own internal records.

3.3.4 Payment Status

Participants **must** use their internal system records to determine the status of payments sent prior to and during the HVCS Fallback Period.

Note: As previously described, receipt of a xsys.002 or xsys.003 response from RITS indicates that a payment has been processed by RITS. Once the SWIFTNet Copy Service has reopened in T-Copy mode, the absence of a xsys.002 or xsys.003 response from RITS indicates that a payment has bypassed RITS. For the avoidance of doubt, payments sent prior to the Disabling Event for which the Sender has received an xsys.002 or xsy,.003 have been settled or rejected and their processing can be considered as complete.

3.4 During HVCS Fallback

3.4.1 Message Format

Senders **must** format messages in accordance with the Bilateral Clearing Form, which contains guidance on how to map the required elements from a pacs.xxx message to the file.

3.4.2 Preventing Non-current Day Payments

Participants **must** ensure that the methods they use for preventing future and back dated payments from being sent in T-Copy and for identifying future and back dated payments received in T-Copy are operating as expected.

3.4.3 Reversing Non-current Day Payments

Senders **must** be responsible for rectifying any future or back dated payments mistakenly sent during the HVCS Fallback Period.

3.4.4 Cash Transfers

Participants **should** send payments that would ordinarily be submitted to RITS through a Cash Transfer as a SWIFT payment, if required.

88 See RITS Member Contingency Procedures (available on the RITS Information Facility) for details.

3.4.5 Projected ESA Balance

Participants **must** use their internal system records to track their bilateral net settlement obligations and projected ESA balance during a HVCS Fallback Period.

3.5 Existing HVCS Fallback

3.5.1 Approaching T-Copy Cut-Off Time

The RBA will send a notification to Participants thirty minutes prior to the Cut-off Time instructing Participants to begin finalising payments.

3.5.2 T-Copy Cut-Off Time

Participants **must** stop sending payments at the Cut-off Time. It is important that Participants do not continue to send payments after this time in order for each Participant to obtain their final bilateral net positions prior to compilation of the HVCS Exchange Summary Form.

3.5.3 SWIFT PDS Reversion

The Company or the RBA will instruct SWIFT to revert the SWIFTNet Copy Service back to Y-Copy mode. This may be lodged in advance of the Cut-off Time but will instruct SWIFT not to action the change any earlier than the Cut-off Time. The SWIFT timings and process for doing this are the same as for the switch to T-Copy performed earlier in the day.

3.5.4 Submit HVCS Exchange Summary Forms

Participants **must** compile their HVCS Exchange Summary Form and submit it to the RBA via email within two hours of the Cut-off Time.

Note: The RBA will consolidate and compare the HVCS Exchange Summary Form submitted by each Participant to generate a Provisional HVCS Exchange Figures Advice for each Participant. Where applicable, the HVCS Exchange Figures Advice will advise a Participant that the amount of a net bilateral obligation they have submitted fails to match the amount submitted by the other Participant (failure to match).

3.5.5 Agree Provisional HVCS Exchange Figures Advice

Participants **should** provide the RBA with email confirmation that they agree to the Provisional HVCS Exchange Figures Advice provided by the RBA at the earliest possible opportunity and by no later than 30 minutes before commencement of the Morning Settlement Session (7am) on the day after the HVCS Fallback Period. Where the HVCS Exchange Figures Advice from the RBA has advised a Participant of a failure to match, the Participant must investigate this and if required, submit a revised HVCS Exchange Summary Form to the RBA before 7am on the day after the HVCS Fallback Period.

Note: From 7am on the day after the HVCS Fallback Period, the RBA will generate and send a Final HVCS Exchange Figures Advice and Net Clearing System Obligations Advice showing a Participant's multilateral net position in the contingency batch, including clearing interest. Where a failure to match remains unresolved, the RBA will apply Failure To Match rules and proceed with the contingency batch.

3.5.6 Failure to Match

The RBA will apply Failure To Match rules in accordance with clause 9.23 of these Procedures if two or more Participants cannot agree on the amount owing for a given obligation.

3.5.7 Reconciliation to RITS

Participants **should** reconcile the internal record of payments (used to calculate their net bilateral obligations) to RITS when RITS recovers.

Note: When RITS is recovered and the system date has rolled forward to the day after the HVCS Fallback Period, the SWIFT Feeder connection is restored. The backlog of HVCS settlement requests stored in the CSI will enter RITS and be rejected due to the back-dated value date. Participants can use the RITS UI to view and export the record of rejected T-Copy payments. Participants can also obtain the record of payments settled or rejected by RITS prior to the Disabling Event using MT950 statements or the RITS UI. Participants can use these RITS records to reconcile the internal records used to calculate the net bilateral obligations submitted to the RBA in the HVCS Exchange Summary Form, which could help to resolve failure(s) to match advised by the RBA in the HVCS Exchange Figures Advice.

Where the reconciliation to RITS cannot be completed before 7am on the day after the HVCS Fallback Period, and the RBA has applied Failure To Match rules in order to proceed with the contingency batch, Participants can continue the reconciliation after the batch has settled and if required, bilaterally arrange the return or correction of a mistaken payment in normal way (in accordance with these Procedures).

3.5.8 ESA Funding

Participants **must** fund any ESA balance shortfall that prevents the contingency batch from settling before the Morning Settlement Session ends.

3.6 Operational Capacity

The following instructions describe the volume of payments that Participants are expected to be operationally capable of processing within the HVCS Fallback Period timeframes.

3.6.1 Payment Volumes

Participants **must** be capable of processing the same volume of payments under T-Copy as they would under Y-Copy. That is, payment volumes must not be reduced during the HVCS Fallback Period because of operational capacity limitations.

Note: For the avoidance of doubt, processing means undertaking the end-to-end steps in the RITS Outage Runsheet which includes exchanging clearing messages in T-Copy, applying funds to Customer accounts, submitting net bilateral settlement obligations to the RBA using the HVCS Exchange Summary Form, and resolving any failure to match discrepancies where required. This requires Participants to ensure the processes they use during a HVCS Fallback Period are scalable for business-as-usual payment volumes.

3.6.2 Staffing

Participants **must** have a pre-determined plan to call on sufficient staff to undertake all steps set out in the RITS Outage Runsheet if a HVCS Fallback Period is declared. Where necessary, this will include non-payment operations staff from the credit, treasury or client account functions, or any other function required by a Participant to facilitate payment exchange during the HVCS Fallback Period.

3.6.3 Timings

Participants **must** be capable of completing all steps set out in the RITS Outage Runsheet within the allocated timeframes.

3.7 Applying Funds

A fundamental objective of the HVCS Fallback Solution is to minimise the potential for systemic disruption during a protracted RITS Disabling Event that could, in extremis, cause financial harm and undermine confidence in the payments system. To achieve this, it is important that Participants actively endeavour to make incoming funds available to Customers prior to deferred interbank settlement occurring the next day. This may require Participants to accept a higher degree of credit risk than when RITS is processing HVCS payments on a RTGS basis.

It should be noted that the HVCS Fallback Solution is intended to be used in the event of a technical disruption to RITS during otherwise normal market conditions. The option to invoke the HVCS Fallback Solution would be assessed at the time considering all relevant factors, including prevailing market conditions. The Company and the RBA could elect not to invoke the HVCS Fallback Solution in adverse conditions where deferred net settlement could give rise to undue risk.

The following section provides instructions and guidance on the extent to which Participants are expected to apply funds to Customers during a HVCS Fallback Period. It makes a distinction between two relevant terms:

(i) *Posting:* a Participant credits the beneficiary Customer's account but does not make the funds available to the Customer until interbank settlement has occurred. Such credits are sometimes referred to as "uncleared funds" and denoted as a visible credit that does not yet form part of the balance of available funds.

(ii) *Availability:* where a *Participant* enables the beneficiary Customer to make use of funds posted to the Customer's account. This could be in advance of interbank settlement occurring.

3.7.1 Posting

Participants **must** post funds received during a HVCS Fallback Period such that the credit entry is visible to the recipient Customer on the same day. With the exception of funds availability, Participants must treat all other aspects of the posting in the same way as normal. This includes interest accruals, which must accrue from the date of clearing not settlement, and returning payments that cannot be applied in accordance with the timeframes in clause 4.20 of these Procedures.

3.7.2 Availability

Participants **should** make a sufficient proportion of total incoming funds available to Customers, so that the objective of the HVCS Fallback Solution can be materially achieved. Decisions concerning the availability of funds is a matter for each Participant and could vary depending on risk appetite, however the expectation is that Participants will maximise the value of funds made available to the greatest extent possible, in accordance with their internal risk appetite. As a guide, achieving the objectives of the HVCS Fallback Solution is estimated to require Participants to make at least 80 per cent of the total value of funds received during a HVCS Fallback Period available to its Customers.

3.7.3 Risk Policy

Participants **must** have an internally agreed risk policy that sets out the approach to meeting instruction 6.7.2 on funds availability during a HVCS Fallback Period. The policy must be documented and approved by the relevant senior personnel; and must be readily available in the event of a HVCS Fallback Period.

Note: The specifics of a Participants' risk policy are entirely a matter for the Participant and could depend on a range of factors including credit appetite, counterparty relationships, net exposures arising from incoming and outgoing settlement obligations; and the value of individual payments received. The policy should contemplate circumstances where Customer's outbound payments are contingent on the availability of funds received. Given the potential time constraints during a HVCS Fallback Period, it may be necessary for Participants to prioritise the assessment of inbound payments that will fund outbound payments due to occur on the same day. As noted, the HVCS Fallback Solution is intended to be used in the event of a technical disruption to RITS during otherwise normal market conditions.

3.7.4 Timely Implementation

Participants **must** be capable of implementing their risk policy during a HVCS Fallback Period, including assessment and approval of credit decisions, within the timeframes set out in the RITS Outage Runsheet.

Note: Participants could consider using a value threshold to determine lower value payments that do not require individual credit assessment before the funds are made available to Customers. For most Participants, a lower bound threshold of $1mn would represent around 90 per cent of total inbound payment volume, but only 2 per cent of total value. Such a threshold could be an operationally efficient approach to prioritising credit decisions for the remaining 10 per cent of payments within the potentially constrained timeframes.

4. Participant Outage Instructions

4.1 Operational Readiness

The following instructions cover items that Participants are expected to have in place in preparation for a Participant Fallback Period.

4.1.1 Operational Readiness

Participants **must** be operationally ready for a Participant Fallback Period. This includes:

1. being familiar with these Procedures and the Contingency Instructions;

2. being capable of making the internal system and operational changes required to send and receive payments during a Participant Fallback Period;

3. participating in contingency test exercises coordinated by the Company; and

4. ensuring staff are available and contactable at all times during the Participant Fallback Period and during planned contingency test exercises.

4.2 Participation

The following instructions describe the extent to which Participants are expected participate in the HVCS when a Participant Fallback Period has been declared.

Instructions for Affected Participant

4.2.1 Sending Payments

The Affected Participant **must** use the Participant Fallback Solution provided for in these Contingency Instructions as the alternative method of sending any payments it considers to be urgent during a Participant Fallback Period.

4.2.2 Participation Opt-Out

Tier 2 Participants that do not intend to use the Participant Fallback Solution if they experience a Disabling Event **must** have pre-agreed this arrangement with the Company. Where there are extenuating circumstances in which a pre-agreed opt-out Participant needs to send payments using the Participant Fallback Solution, the Participant **must** obtain prior agreement from the Company and from the Receiver(s).

Note: A list of the pre-agreed opt-out Participants will be available from the AusPayNet extranet site, such that during a Disabling Event, it is clear to other Participants that a Participant Fallback Period is unlikely to be declared.

4.2.3 Managing ESA Balance

The RBA Domestic Markets Department will contact the Affected Participant where significant deviations in ESA balances are observed.

Instructions for Other Participants

4.2.4 Receiving Payments

All Tier 1 Participants **must** accept payments from an Affected Participant through the Participant Fallback Solution, in accordance with the operational capacity instructions in Section 6.6.

4.2.5 Receiving Payments

All Tier 2 Participants **should** accept payments received from an Affected Participant through the Participant Fallback Solution, in accordance with the operational capacity instructions in Section 6.6. Refusals, if any, **must** be communicated to the Company.

4.2.6 Sending Payments

Participants **must** continue to use the SWIFT PDS for sending payments to the Affected Participant, whilst having regard to the possible liquidity implications and processing delays described in Clause 9.8 of these Procedures. The Participant Fallback Solution provides a means for the Affected Participant to send payments. It cannot be used as a means for the Affected Participant to receive payments outside of the SWIFT PDS.

4.2.7 Pausing Payments

Participants **must**, to the best of their ability, pause sending payments to an Affected Participant if requested to do so by the Affected Participant.

4.3 Entering Participation Fallback

An Affected Participant cannot use the Participant Fallback Solution without prior authorisation from the Company. Authorisation is granted when the Company, or the RBA acting on behalf of the Company, formally declares a Participant Fallback Period.

The key checkpoint times for declaring and entering a Participant Fallback Period are outlined in the Participant Outage Runsheet. In summary, where the Affected Participant's Disabling Event prevents it from sending HVCS payments the priority is to resolve the issue and resume normal operations. If the Disabling Event is not resolved by 15:00 then minimising the delay to payments becomes the priority and the Company, in consultation with the RBA and the Affected Member, could declare a Participant Fallback Period. A Participant Fallback Period could be declared earlier than 15:00 if the Affected Participant has urgent payments to send and cannot estimate their recovery time; or is able to rule out a recovery ahead of the checkpoint times. Decisions concerning a Participant Fallback Period will be communicated to RITS operational contacts via email and SMS.

If the Affected Participant's Disabling Event occurs after 14:00, the Company in consultation with the RBA, would normally expect that a Participant Fallback Period would not be required, but would consider the value of outstanding payments in its assessment.

A Participant Fallback Period will not be declared if the Disabling Event prevents the Affected Participant from using the Participant Fallback Solution.

The following instructions apply once a Participant Fallback Period has been declared.

4.4 Duplicating Participant Fallback

4.4.1 Bilateral Clearing Frequency

The Affected Participant **must** limit the number of HVCS Bilateral Clearing Forms it sends to a Receiver to no more than one every hour, unless agreed with the Receiver.

4.4.2 Payment Volumes

The Affected Participant **must** limit the volume of payments contained in a single HVCS Bilateral Clearing Form to the volumes set out in the operational capacity instructions in section 6.6, unless agreed with the Receiver.

4.4.3 Payment Value Date

The Affected Participant **must** only send value-today payments using Participant Fallback Solution. Future dated payments are not permitted.

4.4.4 Receiver Acknowledgement

The Receiver **must** immediately acknowledge receipt of a HVCS Bilateral Clearing Form from the Affected Participant via encrypted email or phone call to the Affected Participant.

4.4.5 RITS Cash Transfers

The Affected Participant and Receiver **must** each enter a single Cash Transfer for the value of the net bilateral obligation created for each individual HVCS Bilateral Clearing Form exchanged.

Note: If the Affected Participant is unable to access the RITS UI to enter a Cash Transfer, it can contact the RITS Help Desk to request an Assisted Payment. [89]

4.4.6 Settlement Timing

The Affected Participant and Receiver **must** each enter the RITS Cash Transfer and confirm its settlement within 30 minutes of the HVCS Bilateral Clearing Form being sent.

4.4.7 Status Report

The Affected Participant **must** update the RBA and the Company at least every 30 minutes, or as requested, on the status of payments sent using the Participant Fallback Solution and the value and volume of payments outstanding.

Note: The Affected Participant **must** also continue to update the RBA and the Company on the status of the Disabling Event and expected resolution time, in accordance with the RTGS and Retail Payments Incident Reporting Arrangements for RITS Members.

4.4.8 Potential SWIFT Resumption

(a) revert to SWIFT and resolve potential duplicate payments by requesting a Return of Payment from the Receiver; or

(b) hold all outward SWIFT payments and continue using the Participant Fallback Solution.

Note: In accordance with these Procedures, the Affected Participant **must** resume inward payment processing in the shortest possible time. The Affected Participant must consult with the RBA and the Company if holding outward payments will also prevent inward payments processing from resuming.

89 Please see the Assisted Transactions User Guide, available at https://www.rba.gov.au/rits/info/pdf/Assisted_Transactions_User_Guide.pdf

4.4.9 Unexpected SWIFT Resumption

Where the Affected Participant resolves the Disabling Event while the Participant Fallback Solution is in use, and unexpectedly begins to release payments to the SWIFT PDS, the Affected Participant **must** pause all further outward payments processing. The Affected Participant must initiate the request for a Return of Payment for any duplicate payments released, and refer to instruction 6.4.8 on consultation with the Company and the RBA before reverting to SWIFT, or otherwise continue using the Participant Fallback Solution for sending further payments.

4.4.10 Return of Payment

The Affected Participant **must** complete all Return of Payment requests in accordance with Part 4 of these Procedures.

4.5 Exiting Participant Fallback

4.5.1 Cut-off Times

The Affected Participant **must** follow RITS session times and rules when using the Participant Fallback Solution. Meaning:

(a) Outgoing payments from the Affected Participant to Receivers must be sent and settled in RITS by the end of the Settlement Close Session.

(b) Where the Affected Participant is Evening Agreed and wishes to send payments to another Evening Agreed Participant after the Settlement Close Session, the Affected Participant must obtain prior agreement from the Receiver and these payments must be sent and settled in RITS by the Evening Settlement Cut-off.

4.5.2 RITS Extension

The Affected Participant **could** request an extension to the RITS session times. The RBA will, in the normal way, consider the value and volume of payments outstanding in its assessment of whether to grant an extension.

4.6 Operational Capacity

The following instructions describe the extent to which Participants are expected to be operationally capable of sending and receiving payments during a Participant Fallback Period.

4.6.1 Staffing

All Participants **must** have a pre-determined plan to call on sufficient staff to undertake all steps set out in the Participant Outage Runsheet if a Participant Fallback Period is declared.

Instructions for Affected Participant

4.6.2 Bilateral Clearing Forms

The Affected Participant **must** be operationally capable of sending the higher of the following two:

(a) As many HVCS Bilateral Clearing Forms as required to cover at least 80 per cent of its outstanding outgoing transaction value; or

(b) A total of five HVCS Bilateral Clearing Forms per hour, with each form sent to a different Receiver (i.e. five Receivers).

Note: In all cases, the Affected Participant must limit the number of HVCS Bilateral Clearing Forms sent to a single Receiver to no more than one every hour, unless agreed with the Receiver.

4.6.3 Payment Volumes

The Affected Participant **must** be operationally capable of sending at least fifty payments in each HVCS Bilateral Clearing Form and of entering a single RITS Cash Transfer to effect interbank settlement of the bilateral obligation within 30 minutes of the HVCS Bilateral Clearing Form being sent. Fewer than **fifty** payments can be sent if required.

Note: The Affected Participant can increase the number of payments contained in a single HVCS Bilateral Clearing Form if agreed with the Receiver. This recognises that in some cases it may be preferable to send or receive one larger file rather than multiple smaller files.

4.6.4 Payment Values

The Affected Participant **should** be operationally capable of prioritising higher-value payments for inclusion in the HVCS Bilateral Clearing Form. The Affected Participant can include lower-value payments in the HVCS Bilateral Clearing Form if required, subject to this being in accordance with instruction 6.6.2 and 6.6.3.

Note: For most Participants, sending payments greater than $10 million in value will constitute 80 per cent or more of the total outgoing daily transaction value.

Instructions for Other Participants

4.6.5 Bilateral Clearing Forms

The Receiver must be operationally capable of receiving a minimum of one HVCS Bilateral Clearing Form containing at least fifty payments every hour and of entering a single RITS Cash Transfer to effect interbank settlement of the bilateral obligation within 30 minutes of the HVCS Bilateral Clearing Form being received.

4.6.6 Applying Funds

The Receiver **must** be operationally capable of applying payments received in each HVCS Bilateral Clearing Form to Customer accounts on the same day. This includes any screening and downstream processing the Receiver needs to perform prior to applying funds to Customer accounts. For the avoidance of doubt, funds **should** be made available to the Customer for use when the payment is applied to their account.

The next page is Annexure K

ANNEXURE K CYBER FRAUD INSTRUCTIONS FOR THE HIGH VALUE CLEARING SYSTEM[90]

1. Introduction and scope

These Cyber Fraud Instructions are applied under Part 11 of the HVCS Procedures and it provides instructions and guidance for High Value Clearing System Framework Participants in the event that a Framework Participant experiences or is affected by a Cyber Fraud Event. It is intended to adopt a principles-based approach rather than a prescriptive approach in respect of Cyber Fraud Events. The intention is to set a baseline of operational requirements and expectations to enhance the framework's ability to deal with suspected and confirmed fraudulent payments.

Under Regulation 4.12 of the HVCS Regulations, Framework Participants must provide all reasonable assistance to each other Framework Participant and to the Management Committee to investigate any actual or suspected fraudulent activity involving or possibly involving HVCS and identify the source of any fraudulent activity involving HVCS. These Cyber Fraud Instructions are intended to provide guidance on how Framework Participants can provide such assistance to each other.

Framework Participants processing high-value transactions on behalf of a third party ***should*** inform users of their services of the obligation to comply with the Procedures and these Cyber Fraud Instructions.

There are three classifications of instructions:

Rating	**Definition**
Must	Framework Participants are required to implement all 'must' items. These requirements: • refer to the Regulations and other HVCS or SWIFT requirements; • enable Framework Participants to meet their obligations and minimise risk to other members.
Should	Participants are expected to implement 'should' items. These expectations*:* • provide instructions and guidance on aspects of the Cyber Fraud Event that may vary based on the specifics of a Framework Participant's systems or operations.
Could	Participants are encouraged to consider 'could' items but are not required to implement them. These considerations: • provide indications of recommended best practice.

[90] Inserted effective 14/11/22, version 002 r&p 001.22

2. Relationship with other documents

Nothing in these Cyber Fraud Instructions affect a Framework Participant's obligations to comply with the Procedures or the Framework Participant's regulatory and framework requirements.

If a provision of these Cyber Fraud Instructions is inconsistent with a provision of the Procedures, the provisions of the Procedures prevail.

The following documents interact with these Cyber Fraud Instructions.

Document	Relationship / Purpose	Owner
AusPayNet Member Incident Plan (MIP)	Framework for industry coordination during an operational incident affecting the HVCS.	AusPayNet
AusPayNet Crisis Communication Plan (CCP)	Framework for industry and media communication during a major disruption to any of the payments systems or infrastructure that fall under the remit of AusPayNet.	AusPayNet
RITS Member Incident Reporting Arrangements	Arrangements specified by the RBA for reporting by RITS Members during an incident that affects RITS operations, including successful or partly successful cyber-attacks on RTGS or retail payments systems.	RBA
SWIFT Customer Security Program (CSP)	Programme providing support to SWIFT's users in the fight against cyber-attacks and reinforcing the security of the global financial community. Further information available via the SWIFT Knowledge Centre.	SWIFT
SWIFT Recovery Roadmap (SWIFT bulletin 10047)	A SWIFT bulletin providing general advice to SWIFT members on how to respond to a cyber-security incident. Further information available via the SWIFT Knowledge Centre.	SWIFT

3. Definitions and Interpretation

Words defined in the Procedures have, unless the contrary intention appears, the same meaning in these Cyber Fraud Instructions. Otherwise, in these Cyber Fraud Instructions:

Isolation Event means the affected Framework Participant is undertaking the processes set out in SWIFT Recovery Roadmap, which may include suspending the machine, unplugging from the network, shutting down the required ports on the switch or putting the system in an isolated VLAN with an aim to identifying the weakness(es) that resulted in the Cyber Fraud Event. Any questions relating to the processes set out in the SWIFT Recovery Roadmap ***should*** be directed to SWIFT Customer Support.

In these Cyber Fraud Instructions:

(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 word "includes" and "including" is not taken as limiting the meaning of the words preceding it;

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

(e) headings are inserted for convenience and do not affect the interpretation of these Cyber Fraud Instructions;

(f) a reference to a statute or code means the statute or the code, 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, or the provision; and a reference to a specific time means that time in Sydney unless the context requires otherwise.

4. Cyber Fraud Event

Where a Cyber Fraud Event is detected, the affected Framework Participants must review these Cyber Fraud Instructions.

These Cyber Fraud Instructions will not apply if a fraud event does not meet the definition of a Cyber Fraud Event.

Where a Cyber Fraud Event also constitutes a Disabling Event, part 9 of the Procedures and the Contingency Instructions may not apply in all cases, as determined by the Company in the circumstances.

5. Fraud and cyber contacts

Each Framework Participant ***must*** nominate and advise the Company and the System Administrator of a contact point(s) to whom information or enquiries may be directed if a Cyber Fraud Event arises. The Framework Participant ***must*** ensure its nominated contact point(s) remain up to date.

The Company will maintain a list of contact point(s) in Appendix L: Cyber Fraud contacts.

6. Monitoring, testing and maintenance

Pursuant to Regulation 4.9 of the HVCS Regulations, each Framework Participant ***must*** ensure that its own systems and procedures provide appropriate protection against fraudulent activity in connection with HVCS, in accordance with these Regulations and Procedures.[91]

The Management Committee may undertake cyber incident response testing across the HVCS from time to time on reasonable notice. On the Management Committee's request, the Framework Participants ***must*** participate in such testing.

[91] Framework Participants ***could*** consider available market tools that facilitate the case management of fraud payment remediation, which may assist in meeting this obligation and ensuring the timely identification and remediation of payment fraud.

7. Notification and reporting requirements

On becoming aware of a Cyber Fraud Event:

(a) A Sender that causes or may cause the Cyber Fraud Event:

(i) ***must*** report the Cyber Fraud Event in accordance with the requirements to report successful and near-miss cyber-attacks specified in the RITS Member Incident Reporting Arrangements (if applicable); and

(ii) ***must*** report the Cyber Fraud Event to the Company in accordance with Regulation 4.10 of the HVCS Regulations (if applicable), and ***must*** comply with the reporting requirements indicated in the CCP or MIP (if applicable); and

(b) A Receiver that is or may be affected by a Cyber Fraud Event (eg Receivers of confirmed or suspected fraudulent payments):

(i) ***should*** report the ***Cyber*** Fraud Event to the Company in accordance with Regulation 4.10 of the HVCS Regulations (if applicable); and

(ii) ***should*** notify the Sender ***where*** the Sender may not already be aware of payments the Receiver has identified as suspicious through its own screening. The Sender can be notified using the applicable contact point(s) maintained in Appendix L or via the Company.

8. Obligations of Receivers

If a Receiver that is affected by or potentially affected by a Cyber Fraud Event (eg a Receiver becomes aware that it has received payment arising from a Sender that is the subject of a Cyber Fraud Event), it ***should*** freeze and hold suspected fraudulent payments if requested by the Sender and/or the Management Committee. This does not apply if the Sender requests for Return of a Settled Payment Sent in Error, in accordance with clause 4.20 of the Procedures.

9. Obligations of Senders

If a Sender that causes or may cause a Cyber Fraud Event, it (on becoming aware):

(a) ***must*** immediately assess steps are appropriate to be undertaken in the circumstances to prevent or reduce the likelihood of other fraudulent or potentially fraudulent payments from being transmitted through the SWIFT PDS and action these steps. For example, it ***could*** remove itself from the SWIFT PDS CUG by initiating an Isolation Event or undertake other appropriate action;

(b) ***must*** comply with directions received from the System Administrator in relation to the Cyber Fraud Event (if any); and/or

(c) ***must*** comply with directions from the Management Committee in relation to the Cyber Fraud Event, including a direction to initiate an Isolation Event.

While the Isolation Event is active, the Sender that is isolating will not be able to send or receive any HVCS payment processing.

10. Exiting an Isolation Event

Prior to exiting an Isolation Event, the Sender that that is isolating a Cyber Fraud Event ***must***:

(a) provide assurance to the Management Committee that the cause of the Cyber Fraud Event has been resolved. This may include providing the Management Committee with relevant information about the Cyber Fraud Event and the Isolation Event, including a description of the control failures that enabled the Cyber Fraud Event, what rectification measures have been applied, any independent verifications and controls reviews undertaken, details of penetration testing and any other information as may be appropriate in the circumstances or as otherwise requested by the Management Committee;

(b) ensure the authenticity and integrity of payments queued in the Framework Participants SWIFT systems have been checked prior to reconnection to the SWIFT PDS; and

(c) if requested by the Management Committee, heighten its monitoring and screening of payments for a specified period of time after reconnection.

The Isolation Event will continue until the Management Committee notifies the Framework Participant experiencing the Cyber Fraud Event that it has provided sufficient assurance to Management Committee (acting in its sole discretion) that the cause of the Cyber Fraud Event have been identified and addressed to prevent any further impact to other Framework Participants or risk to the integrity of the HVCS.

11. Powers and Duties of the Management Committee

The Management Committee can exercise its powers as set out in the HVCS Regulations.

12. Framework Participants' Liability in a Cyber Fraud Event

Framework Participants' liability is as set out in Regulation 4.11 of the HVCS Regulations.

The next page is Annexure L

ANNEXURE L CYBER FRAUD CONTACTS[92]

Appendix L is located separately

-- END --

[92] Inserted effective 14/11/22, version 002 r&p 001.22