eftpos Technical, Operational and Security Rules

Version 2.22

Version 2.22 effective 22/10/2024

eftpos

Good for Australia

Copyright and disclaimer

Information in this document is the confidential information of eftpos Payments Australia Limited and is subject to change without notice.

No part of it may be copied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior written permission from eftpos Payments Australia Limited.

Written and published in Sydney, Australia by eftpos Payments Australia Limited.

ABN 37 136 180 366

Document control

Amendment history

Version	Date	Key changes
0.2.1	21 Sep 2010	Review prepaid sections
0.2.2	29 Sep 2010	Progression of the above and interaction with CECS rules.
0.3.1	3 Nov 2010	Change of abbreviated name from TOS rules to Operational Rules. Identification of Confidential clauses.
1.0	7 Dec 2010	As approved by Board on 07/12/10.
1.1	11 Oct 2011	• Changes to Section 8. • Addition of eftpos batch file format and reporting requirements in new Part 11. • Amendments to floor limit for cash or cash/purchase combined transactions.
1.2	16 Apr 2012	• As approved by Board Updated requirements for eftpos fee code in F047 for 0200/0220 messages. • As per Member Advice 006-12, Changed field length for F025 in the 0200 and 9200 messages from 3 to 2. • Changed reference to standard for F018 to Merchant category code AS2805 part 16. • Added 11C.1.6 Technical Contacts. • Removed footnote 7 for F04 of 0200 message as it relates to ATM direct charge. • AmendedF028 footnote as the field is used for ATM fees. • Removed references to “common fields” section and ensured all fields referenced are contained in the Fields section of Appendix 5I. • Corrected field length for F055 Tags 9F26 and 9F27. • Removed reference to AS3521 Identification cards - Physical characteristics standard withdrawn.
1.3	31 Oct 2012	• As approved by the Board 4 October 2012. • 1.2 Amended definition for Service provider. • 8.5.3 Replaced transaction diagram and amended description for eftpos cash out as it contained ATM processing information. • 6.4.1 Fees. Added details of where fees are published. • 11.1 & 11.3.3 Added clauses for reporting of data breach or compromise. • 11.2 Added clauses relating to disclosure of reporting information. • 3A.3 Severity Levels. Minor edits. • 3A.5 Added notifications received by the company.

Version	Date	Key changes
		• 3A.6 Added Post Incident outage report. • 6B.1.7 Added File compression. • 6c.1.2 Corrected reference from SHA-2 to SSH-2. • 6C.1.7 Amended contact details for technical staff.
1.4	1 May 2013	• 5.12.5, 6.1.1, 6.1.2, 6.1.3, 8.9.1, 11.3.1, 11.3.2&6C.1.3 Minor edits and corrections. • 6B.1.8, 6B.1.9&6B.1.10Amended field description of Field 11 Systems Trace Audit Number (STAN), to reflect the field description in the Original message. • 6B.1.8, 6B.1.9, 6B.1.10&6B.1.11Amended field description of Field 15 Settlement date, to reflect the field description in the Original message.
2.0	15 Apr 2014	• Document restructured for eftpos Chip and Contactless processing. • Added definitions for Chip and Contactless. • Amended references to message format to include Appendix 5 for bilateral messages and the eftpos Hub Link Specification document for eftpos Hub direct connectors including Chip and Contactless messages. • Amalgamated all fallback and dispute sections to 2.7 Common requirements. • Updated limits and fallback types to include eftpos EMV fallback processing. • Document restructured and definitions added for the introduction of the eftpos Hub and the incorporation of the eftpos Access Code connectivity arrangements into the eftpos Scheme Rules. • Deleted contingency file processing as not supported by Members. • Updated registration and certification requirements to support eftpos Chip and Contactless processing. • Clarified requirements for Cash and Cash/Purchase transactions.
2.1	1 Oct 2014	• Clarification of requirements for short duration pre-authorisation transactions. • Change requirement for F55 in batch file reporting to optional. • Added definitions for TAV and CTAV. • Updated document names referenced in the manual. • Minor amendments requiring Acquirers to provide merchants with guidelines for processing cash out and surcharges. • Minor clarifications to some clauses for unattended devices • General corrects/edits for typographical errors and cross references.
2.2	1 Apr 2015	• Version 2.1 Re-published without change.
2.3	1 Nov 2015	• Restructure of TOSR document. • Changes to add requirements for eftpos Digital for eftpos Online. • Rewrite of Disputes and Chargebacks Section. • Updates to Reporting requirements.
2.4	28 April 2016	• Introduction of requirements for eftpos Mobile.

Version	Date	Key changes
		- Introduction of tokenisation requirements.
2.5	26 October 2016	- Minor and technical changes regarding: – eftpos Chip and Contactless – eftpos Mobile and Tokenisation – Changes to regulatory requirements - Other minor changes and clarifications
2.6	27 April 2017	Changes for: - Updates to eftpos Mobile - Introduction of eftpos Settlement Service - Introduction of support for eftpos In-App - Updates to Disputed Transactions and Chargebacks
2.7	25 October 2017	Changes for: - In-App Payments to support Refund Transactions - Clarification for Cashout support across interfaces - Issuer support for default account - Updates to eftpos Settlement Service following RBA feedback - Updates to Disputed Transaction and Chargebacks reporting - Other minor changes and clarifications
2.8	25 April 2018	Changes for: - Introduction of eftpos Digital Acceptance (formerly eftpos Online) through the eftpos Digital Acceptance Framework. - Updates to Disputed Transactions and Chargebacks to address card not present transactions. - Addition of a Corrective Batch as part of eSS. - Updates to requirements for certification of eftpos Acceptance Devices. - Updates to the eftpos Certification Body pre-requisites for Acceptance Devices. - Removal of Bilateral Interchange Specification.
2.9	24 October 2018	Changes for: - Clarifications relating to eftpos Digital Acceptance, as a result of eftpos Digital Acceptance Reference Group feedback. - Introduction of eftpos Open Loop Transit. - Additional requirements relating to Merchant routed transactions. - Clarifications relating to Acceptance Devices, Cashout and Fallback processing. - Clarification of eftpos Disputed Transactions and Chargebacks reason codes.

Version	Date	Key changes
		• Amendments to bilateral Interchange Link and bilateral Settlement provisions.
2.10	30 April 2019	Changes for: • Introduction of Merchant Token Requester, Merchant Initiated Transactions and Staged Digital Wallets (eDAF) • Clarification of eftpos Disputed Transactions and Chargebacks. • Clarifications relating to Acceptance Devices, Cashout and Fallback processing. • Amendments to bilateral Interchange Link and bilateral Settlement provisions. • Other summary minor and technical corrections.
2.11	07 July 2019	Changes for: • Requirement regarding CNP Fraud rates - AusPayNet CNP Framework • Updates to support new eftpos Digital use cases • Updates to Member obligations regarding the Service Providers • Updates to support Open Loop Transit transactions on eftpos Form factors. • Updates to cater for Consumer Data Right regulations
2.12	05 May 2020	Changes for: • Inclusion of requirements for BIN Controller for allocating PARs to the eftpos proprietary cards. • Updates to Authorised eftpos Digital Merchant requirements • Initial introduction of terms around transaction fraud data reporting requirement for Issuers.
2.13	12 Feb 2020	Changes for: • Updates to eftpos Digital transactions acceptance – MTR mandate dates for MND & prop. cards. • 3DS fraud liability shift dates for MND & prop cards
2.14	27 Oct 2020	Changes for: • 3DS fraud liability shift dates for MND & prop cards • Introduction of eftpos API Platform for accessing various eftpos Services.
2.15		Changes for: • eSS Enhancements • Digital Taxonomy • Digital Card not Present (CNP) • eftpos Secure
2.16		Changes for:

Version	Date	Key changes
		• Introduction of eftpos Co-brand card. • eftpos API Gateway • Incorporating Digital Card Not Present (CNP) mandates approved by the eftpos Board • eftpos Secure
2.17	Apr 2022	Changes for: • CNP Deposit and Withdrawal; and • Digital Taxonomy tidy-up
2.18	07 Apr 2022	Changes for • Prepaid – Reloadable Ace • Dispute and Chargebacks – Pre-arbitration • Tag MCR – Optional • Digital Acceptance changes – section 4.7.10.8 • Align with Consolidation changes
2.19	20 Jan 2023	Changes for: • Clarifications for eftpos Digital Acceptance • Fraud and Chargebacks monitoring and reporting • mPOS • eQR (note that the clauses relating to eQR have not been ratified and are not yet applicable to Members)
2.20	30 Jun 2023	Changes for: • Alignment with Australian Payments Network Device Approval Process • Cashout • Manual imprinters Clarification for: • eftpos Mobile • Merchant Choice Routing • eftpos Digital – support models for Instalment Service Providers;
2.21		Changes for: • Additional option for obtaining a new AIN • Clarity on Offline limits for Multi Network Cards • eQR Tokenisation device binding • eQR support for Switch to Acquirer (S2A) payment processing • Acquirer requirements and definitions for Payment Facilitators and Marketplaces • Clarification on Fast Notification Payment Advices for S2I

Version	Date	Key changes
		- Removal of EMV Phase 1 requirements
2.22	30 June 2024	Changes for: - Token cryptograms - Clarification for Payment Facilitators - Minor updates to definitions.

Table of contents

1. Overview

1.1. Scope of these Rules

These Technical, Operational and Security Rules are prescribed by the Company under the Scheme Rules.

Standard Hub Direct Connections:

The requirements for a Standard Hub Direct Connection are set out in this document and the Standard Hub Service Schedule which is incorporated into and forms part of these Technical, Operational and Security Rules in respect of Direct Connections to the eftpos Hub. To the extent of any inconsistency between this document and the Standard Hub Service Schedule, the Standard Hub Service Schedule prevails in respect of Direct Connections to the eftpos Hub.

Direct Connection to the eftpos TSP:

The requirements for a Direct Connection to the eftpos TSP are set out in this document, the Mobile Service Schedule and eTS-F Service Schedule which are incorporated into and forms part of these Technical, Operational and Security Rules in respect of Direct Connections to the eftpos TSP. To the extent of any inconsistency between this document and the Mobile Service Schedule or the eTS-F Service Schedule, the respective service schedule prevails in respect of Direct Connections to the eftpos TSP.

eftpos Settlement Service:

This document sets out the requirements for the Settlement of eftpos Transactions, including Failure to Settle (FTS) procedures.

Direct Connection to eftpos Services, including Hub and TSP, via the eftpos API Gateway:

The requirements for a Direct Connection via the eftpos API Gateway are set out in this document and the API Gateway Services Schedule which is incorporated into and forms part of these Technical, Operational and Security Rules in respect of Direct Connections to the eftpos. To the extent of any inconsistency between this document and the API Gateway Services Schedule, the API Gateway Services Schedule prevails in respect of Direct connections to the eftpos API Gateway.

Direct Connection to eftpos Secure Directory Server:

The requirements for a Direct Connection to the eftpos Secure Directory Server are set out in this document and the eftpos Secure Service Schedule which is incorporated into and forms part of these Technical, Operational and Security Rules in respect of Direct Connections to the eftpos Secure

Directory Server. To the extent of any inconsistency between this document and the eftpos Secure Service Schedule, the eftpos Secure Service Schedule prevails in respect of Direct Connections to the eftpos Secure Directory Server.

1.2. Purpose of these Rules

These Technical, Operational and Security Rules apply to eftpos Transactions and any other activity, processed using the eftpos Hub, eTSP or other eftpos infrastructure.

Other standards and documents may be incorporated by reference to these Technical, Operational and Security Rules. If this is done, Members must comply with those standards and documents to the extent that they are incorporated by reference.

2. Common requirements

2.1. Identification of Issuers

Each Issuer must be registered in accordance with AS 3523.2 which specifies the application and registration procedures for Issuer Identification Numbers (IIN) in accordance with AS 3523.1. In line with industry practice, IINs are referred to as BINs in these Technical, Operational and Security Rules. BINs for use within the eftpos Payment System are set out at clauses 3.8 and 3.9.

2.2. Identification of Acquirers

Acquirers must be identified by an Acquirer Identification Number which is a unique number allocated to the Acquirer by eftpos. The Acquirer may also use an Acquirer Identification Number allocated by the International Organisation for Standardisation (ISO). Where the Acquirer is also an Issuer, the Member's BIN allocated in relation to its eftpos debit cards may be utilised as the Member's Acquirer Identification Number (AIN). All transactions routed via the eftpos Hub must use an AIN agreed for such use with eftpos, and that AIN must represent an eftpos Member. The AIN must be populated by the Acceptance Device in all eftpos Transactions.

2.3. eftpos Certificate Authority

Members must follow the eftpos Certificate Authority process and procedures as published by the Company from time to time prior to:

- issuing eftpos Form Factors; and/or
- deploying Acceptance Devices
- connecting to eftpos Secure Directory Server.

2.4. Compliance and certification of eftpos Form Factors, Acceptance Devices and eftpos Hub Direct Connections

The following must comply with and be certified as compliant with the relevant eftpos specifications as published from time to time by eftpos, in accordance with eftpos Certification Body requirements as set out in the published eftpos Certification Body documentation before issuance, deployment or establishment of connectivity respectively:

a. Cards and other eftpos Form Factors carrying an eftpos applet or other eftpos applications used in eftpos Transactions; and

b. Acceptance Devices used with eftpos Form Factors. All devices must also have pre-requisite approvals as outlined in the eftpos Certification Body Certification Services document.

c. Direct Connections to the eftpos Hub as specified in the Standard Hub Service Schedule, Mobile Service Schedule, and the Standard Direct Connection Project Documents, before being placed into production, and before production implementation by the Direct Connector of each biannual compliance release.

d. Direct Connections via the eftpos API Gateway as specified in the API Gateway Services Schedule, before being placed into production, and before production implementation.

e. Direct Connectors for eftpos Secure as specified in the eftpos Secure Service Schedule, before being placed into production, and before production implementation.

2.5. Approved Devices

2.5.1 Security

All Secure Cryptographic Devices utilised by Members (or on behalf of Members) and engaged in eftpos Interchange Activities are required to have been evaluated and approved according to the following:

a. for eftpos Terminals:

i. The PCI PIN Transaction Security (PTS) Point of Interaction (POI) requirements; or

ii. The PCI MPoC (CPoC / SPoC) solution requirements; or

iii. The Australian Payments Network Process for Considering Non-Standard Technologies at the Point of Interaction (where PCI PTS is not applicable) ; or

iv. The Australian Payments Network IAC Device Approval Process.

b. for SCMs, Australian Payments Network's IAC Code Set.

If requested to do so by the Company, a Member must produce an approval letter for each Secure Cryptographic Device and configuration that it has implemented.

Members with eftpos Terminals on the Australian Payments Network Expired Devices List must meet the conditions published by Australian Payments Network for the device to remain approved. A device must not continue to be used once the sunset date has passed.

Additional guidance regarding approved eftpos Terminals is set out in the eftpos Terminal Device Security Guide.

2.6. Compliance programs

To ensure the security and integrity of the eftpos network, Members with a direct contractual relationship with the Company using Schedule 4 of the Scheme rules are required to undertake the compliance programs and co-operative measures referred to in this section.

2.6.1 Annual Security Audit programs

The Annual Security Audit Program is an annual requirement designed to ensure that uniform security audit procedures are applied among all Members. To be effective, all entities involved in the processing of PINs from its entry at the eftpos Terminal up to and including its delivery to the Issuer's authorisation processor must adhere to an agreed set of procedures and adopt a common audit process to ensure adherence to those security procedures.

The Company will notify Members of the outcomes of any compliance audit performed on third party service providers engaged by the Company in the provision of services for Members.

2.6.1.1 PIN Security compliance

All members as indicated in the Clause 1.8 of Scheme Rules must evidence compliance with the Security requirements by completing and submitting to the Company a Security Compliance Checklist (satisfactory to the Company) to confirm that they are able to, and do, meet the device security and management standards in force at the time, including that:

a. only approved SCDs are employed in eftpos Interchange or to manage Keys or PINs used in interchange.

b. the management of the SCD meets the applicable Security Management Standards (see section 5.

c. the key management practices employed comply with current AS 2805 part 6 requirements.

d. PIN management procedures and practices comply with current AS 2805 part 3 requirements; and

e. PIN change over open network procedures and practices comply with Volume 2 of the IAC Code Set.

2.6.1.2 Timing of Security Audit

Members must complete a Security Compliance Checklist once every calendar year with the period between submitting the checklists being no less than 9 months and no longer than 15 months.

2.6.1.3 Security Compliance checklist

The Security Compliance Checklist specified by the Company must be used for the annual compliance statement. It must be signed by the Member and countersigned by its either internal auditor or an external auditor.

2.6.1.4 Australian Payments Network IAC participation

Unless the Company directs otherwise, if a Member is also an IAC participant, then it may satisfy the Security Audit Program obligations above by producing evidence of compliance with the Australian Payments Network's Security Audit Program annually. The Member must notify the Company if the Member will take advantage of this clause 2.6.1.4.

2.6.2 eftpos annual compliance

eftpos Members in their own right and on behalf of Direct Connectors and Service Providers must ensure compliance with mandates and milestones as notified from time to time by completing and submitting the Compliance Self-certification checklist (as supplied by the Company) no less than once annually at such time as notified by the Company each year in accordance with the processes and procedures published by the Company from time to time.

2.7. Privacy co-operation

Each Member must co-operate with each other Member and the Company, and parties authorised by an eftpos Consumer in the fulfilment of their respective obligations under Privacy Laws and other Laws impacting Consumer Data, such as, without limitation;

a. including required collection information for other parties involved in Provisioning of eftpos Form Factors, processing eftpos Transactions, processing authentication messages within eftpos Secure and the resolution of Disputes and Chargebacks;

b. providing notification to the Company and any other Member, if the Company or another Member is impacted by a serious Notifiable Incident, originating from the notifying Member. Notification is required to be provided in the manner and timeframes set out in the Privacy Act and at clause 9.1.6 of these Technical, Operational and Security Rules.

This provision does not apply to the extent that it would put a Member in breach of their obligations under applicable privacy legislation.

2.8. Network and Interchange requirements

2.8.1 Direct Connections overview

2.8.1.1 Service levels and operating requirements

The service levels and operational requirements for the eftpos Hub are set out in:

a. these Technical, Operational and Security Rules;

b. the Standard Hub Service Schedule;

c. the eftpos Hub Link Specification and eftpos Hub File and Reports Specification;

d. the relevant sections of the IAC Code Set as identified in this document, provided that in respect of Settlement, the IAC Code Set ceases to apply to Settlement of eftpos Transactions from the date specified in a notice from the Company to Members as the effective date from when the eftpos Settlement Service referred to in Part 8 is operational; and

e. the COIN Operating Manual.

The service levels and operational requirements for the eftpos TSP are set out in:

a. these Technical, Operational and Security Rules;

b. the Mobile Service Schedule;

c. the eftpos eTS-F Service Schedule

d. the relevant eLS Token Management Addendum;

e. the eftpos Issuer Web Service Tokenisation API specification; .and

f. the eftpos API Specification

Each Member and each Direct Connector to the eftpos Hub must meet the service levels and operational requirements for a Standard Hub Service Direct Connection set out in:

a. these Technical, Operational and Security Rules;

b. the Standard Hub Service Schedule and eftpos Hub Link Specification;

c. the relevant sections of the IAC Code Set as identified in this document, provided that in respect of Settlement, the IAC Code Set ceases to apply to Settlement of eftpos Transactions from the date specified in a notice from the Company to Members as the effective date from when the eftpos Settlement Service referred to in Part 8 is operational; and

d. the COIN Operating Manual -if they are a member of COIN.

Each Member and each Direct Connector to the eftpos TSP must meet the service levels and operational requirements for a Direct Connection to the eftpos TSP set out in:

a. these Technical, Operational and Security Rules;

b. the Mobile Service Schedule;

c. the eftpos eTS-F Service Schedule

d. the relevant eLS Token Management Addendum;

e. the eftpos Issuer Web Service Tokenisation API specification; and

f. the relevant eftpos API Specifications.

Each Member and each Direct Connector to the eftpos API Gateway must meet the service levels and operational requirements for a Direct Connection to the eftpos API Gateway as set out in:

a. these Technical, Operational and Security Rules;

b. the API Gateway Services Schedule;

c. the respective service schedule applicable to the eftpos Infrastructure to which the Direct Connector has a Direct Connection; and

d. the eftpos API Specifications.

Each Member and each Direct Connector to the eftpos Secure Directory Server must meet the service levels and operational requirements for a Direct Connection to the eftpos Secure Directory Server as set out in:

a. these Technical, Operational and Security Rules;

b. the eftpos Secure Services Schedule;

c. the relevant eftpos Secure Specifications; and

d. the relevant eftpos Secure Implementation Guides.

2.8.1.2 Security requirements

Direct Connectors to the eftpos Hub must, at a minimum, comply with the security requirements in Part 2 of the COIN Operating Manual and PCI DSS in respect of Interchange Links, through a Standard Hub Service.

Direct Connectors to the eftpos TSP must, at a minimum, comply with the security requirements in the Mobile Service Schedule, e-TSF Service Schedule and PCI DSS in respect of the interface to the eftpos TSP.

Direct Connectors to eftpos API Gateway must, at a minimum, comply with the security requirements in the eftpos API Gateway Services Schedule.

Direct Connectors to eftpos Secure Directory Server must, at a minimum, comply with the security requirements in the eftpos Secure Services Schedule.

The Company will comply with the security requirements in Part 2 of the COIN Operating Manual and maintain PCI DSS certification in respect of the eftpos Hub (noting that the eftpos TSP is hosted within the eftpos Hub environment).

Each Direct Connector must manage their own users of any access to any infrastructure or application used for the purposes of the Direct Connection in accordance with best practice security methods including without limitation PCI DSS.

2.8.1.3 Project and implementation process

The project and implementation process for a Direct Connection to the eftpos Hub is as set out in the Standard Hub Service Schedule.

The project and implementation process for a Direct Connection to other eftpos Infrastructure as set out in the respective service schedules.

2.8.2 Responsibility

The eftpos network comprises many components with Members responsible for managing their own components that make up the network. Responsibilities for the various components of the network are:

Component	Responsibility
PEDs/eftpos Terminals	Acquirer
eftpos Terminal to Host communications	Acquirer

Component	Responsibility
Acquirer Host / Acquirer SCM **(including any Direct Connector or Processors engaged to provide services to the Acquirer)**	Acquirer
Interchange Line / Interchange Link direct between Members, whether or not through the COIN	Shared responsibility of the two Members involved if a direct link between Issuer and Acquirer.
Interchange Link/Interchange Link between Direct Connector and eftpos Hub	Shared responsibility of the Direct Connector and the Company for Direct Connections to the eftpos Hub.
Issuer Host / Issuer SCM **(including any Third Party Processors engaged to provide services to the Issuer)**	Issuer
eftpos Hub	The Company
eftpos TSP	The Company
Interface between a Direct Connector or Member and the eftpos TSP	Shared responsibility of the Direct Connector and the Company
eftpos API Gateway	The Company
Interface between a Member or Direct Connector and eftpos API Gateway	Shared responsibility of the Member/Direct Connector and the Company
eftpos Secure Directory Server	The Company
Interface between a Direct Connector or Member and the eftpos Secure Directory Server	Shared responsibility of the Member/Direct Connector and the Company

Table 1: Network component responsibilities.

For Standard Hub Direct Connections network and Interchange requirements, see Standard Hub Service Schedule and for connections to any other eftpos Infrastructure, are as set out in the respective service schedules.

2.8.3 Time-out values

The standardisation of time-out values used across the eftpos network ensures consistent customer experiences in circumstances where there is disruption to normal processing.

The time-out values for Standard Hub Direct Connections are set out in the Standard Hub Service Schedule and eftpos Hub Link Specification.

The time out values for API Direct connections are set out in eftpos API Gateway Services Schedule.

The time out values for Direct connections to other eftpos Infrastructure are set out in the respective service schedules.

2.8.4 Disablement of connections

2.8.4.1 No longer used

2.8.4.2 Disablement of Direct Connections by the Company

A Direct Connector may request that the Company disable a Standard Hub Direct Connection in respect of another Direct Connector where excessive response times or message volumes from that other Direct Connector are causing a degradation of the service levels achieved by the requesting Direct Connector through the eftpos Hub. The Company may, at its discretion and in accordance with this clause 2.8.4.2, disable a Standard Hub Direct Connection.

Subject to clause 24.2 of the Scheme Rules, an Issuer may also direct the Company to configure the eftpos Hub to deny eftpos Transactions from certain specified BINs.

A Direct Connector may temporarily disable one link within its own Direct Connection to the eftpos Hub:

a. following prior notice to the Company and the eftpos Hub Service Provider;

b. for maintenance of that one link, provided that:

   i. maintenance of all links within that Direct Connector’s Direct Connection do not occur simultaneously; and

   ii. the remaining link or links continue to meet the service levels required by the Standard eftpos Hub Service Schedule for the proposed duration of the disablement;

c. if required to address congestion over one or more links within a Direct Connections, for example, where eftpos Transaction response times or eftpos Transaction volume received from those Direct Connections are regularly and frequently exceeding published service levels; and

d. provided that full processing of eftpos Transactions through the Direct Connection is restored within the required Restoration Period.

The Company may temporarily disable one or more links within a Direct Connection to the eftpos Hub:

a. on notice to the impacted Direct Connector;

b. for maintenance of that one or those links, provided that:

   i. maintenance of all links within that Direct Connector's Direct Connection to the eftpos Hub do not occur simultaneously; and

   ii. the remaining link or links continue to meet the service levels required by the Standard eftpos Hub Service Schedule for the proposed duration of the suspension;

c. if required to address congestion over one or more Direct Connections, for example, where eftpos Transaction response times or eftpos Transaction volume received from those Direct Connections are regularly and frequently exceeding published service levels in the Standard Hub Service Schedule;

d. for product development or implementation of an eftpos Development Project; and

e. provided that full processing of eftpos Transactions through the Direct Connection is restored within the required Restoration Period.

Such disablement shall be accomplished either at the network layer or application layer.

If an Issuer is disabled then the eftpos Hub will return the appropriate response in accordance with the eftpos Hub Link Specification and any applicable Acquirer Fallback procedures will apply.

If an Acquirer is disabled then the Acquirer host may return the appropriate response in accordance with the eftpos Hub Link Specification to its connected eftpos Terminals and Acquirer Fallback procedures will apply.

The Company may temporarily disable a Direct Connection to the eftpos TSP:

a. on notice to the impacted Direct Connector;

b. for maintenance;

c. for product development or implementation of an eftpos Development Project; and

d. provided that full availability is restored within the required restoration period as set out in the Mobile Service Schedule and eTS-F Service Schedule.

Such disablement shall be accomplished either at the network layer or application layer.

If an Issuer is disabled then the eftpos TSP will return the appropriate response in accordance with the eftpos Hub Link Specification.

The Company may temporarily disable a Direct Connection to the eftpos API Gateway:

a. on notice to the impacted Direct Connector

b. for maintenance

c. for product development or implementation of an eftpos development project;

d. provided that full availability is restored within the required restoration period as set out in the eftpos API Gateway Services Schedule; and

e. if it deems that the entity connecting to the eftpos portal is not utilizing the portal for its intended use. The Company may disable a specific service and/or access to entire eftpos API Gateway as eftpos in its discretion deems necessary.

Such disablement shall be accomplished either at the network layer or at the application layer.

If a member or Direct Connector is disabled, then the eftpos API Gateway will return the appropriate response in accordance with the respective API specifications.

The Company may temporarily disable a Direct Connection to the eftpos Secure Directory Server:

a. on notice to the impacted Direct Connector:

b. for maintenance

c. for product development or implementation of an eftpos development project;

d. provided that full availability is restored within the required restoration period as set out in the eftpos Secure Service Schedule; and

e. if it deems that the entity connecting to the eftpos Secure Directory Server is not utilising the eftpos Secure Directory Server for its intended use, the Company may disable a specific service and/or access to the eftpos Secure Directory Service as eftpos, in its discretion deems necessary.

Such disablement shall be accomplished either at the network layer or at the application layer.

If a member or Direct Connector is disabled, then the eftpos Directory Service will return the appropriate response in accordance with the respective EMVCo 3DS Specification. Further details are covered in the eftpos Secure Service Schedule.

2.9. Interchange Technical Specifications

The eftpos Hub Link Specification (eLS) will apply to all Interchanges through a Direct Connection to the eftpos Hub.

The eftpos API Specifications shall apply to Member and Direct Connector connectivity with and between the API Gateway and the eftpos Payment System.

2.9.1 Dialogue

Unless otherwise specified by the Company, a two-message dialogue will be used across the Interchange Link.

2.9.2 Communications Protocol and line configuration

Direct Connectors to the eftpos Hub must, at a minimum, comply with the requirements in the COIN Operating Manual, through a Standard Hub Service. The Company will comply with the communications protocols and line configuration requirements in the COIN Operating Manual in respect of the eftpos Hub.

Direct Connectors using the eftpos API Gateway must comply with the requirements specified in eftpos API Gateway Services Schedule.

2.9.3 Message formats

Messages exchanged with the eftpos Hub and eftpos TSP must be formatted according to the eftpos Hub Link Specification and relevant eLS Addendums or in the case of Direct Connectors using the eftpos API Gateway, comply with eftpos API Specifications.

2.9.4 Reconciliation messages

The exchange of reconciliation messages will be within 10 minutes from the agreed cutover time. These reconciliation messages will relate to all Transactions where the request/advice message bears a date consistent with the data being settled.

2.9.5 Sign On

Direct Connections to eftpos Hub will Sign On according to the eftpos Hub Link Specification or in the case of Direct Connectors using the eftpos API Gateway, comply with eftpos API Specifications.

2.9.6 Messages

The supported message types are defined in:

a. clause 6.3;

b. eftpos Hub Link Specification;

c. eftpos API Specifications; and

d. eftpos Issuer Web Service Tokenisation API specification.

2.9.7 Redundancy

Direct Connectors to the eftpos Hub through a Standard Hub Service must comply with the Standard Hub Service Schedule in respect of redundancy.

The eftpos Hub will run in active/active configuration for eftpos Transaction processing with an additional disaster recovery site for the back office. The eftpos TSP will run in an active/active configuration for Tokenisation services, and in an active/hot standby configuration for Provisioning.

Direct Connectors using the eftpos API Gateway must comply to eftpos API Gateway Services Schedule in respect of redundancy.

2.9.8 Acceptance Device details

Transaction messages must contain Terminal or Merchant name, location (or in the case of eftpos Digital Acceptance, Transaction reference) and Card Acceptor Terminal ID (including a unique identifier provided in the absence of a physical Terminal) to enable completion of statement narratives.

If a Payment Facilitator applies one or multiple Card Acceptor Terminal IDs across all terminals in their fleet, or one or multiple Card Acceptor Identification Codes (Merchant IDs) across all End Merchants for Form Factor Present Transactions, both the Acquirer and the Payment Facilitator will be required to utilise the proprietary unique identifier (e.g. the End Merchant Identifier assigned by a Payment Facilitator) to uniquely identify an End Merchant based on their specific business model and appropriate risk controls as required in Clause 4.7.14.

2.10. Third party Service Provider checks

Third party Service Providers (including Processors) are engaged by Members to provide services or perform functions within the eftpos Payment System that would normally have been provided by the Member. As such, Members are responsible for the actions of third party Service Providers when engaged in any connection with the eftpos Infrastructure on behalf of the Member including but not limited to eftpos Transactions on behalf of the Member. For this reason, Members must include any services provided to the Member by the third party Service Providers in the Members Annual Security Audit and Certification Checklist. Acquirer Members must ensure that any Merchant utilising the services of a Merchant's Service Provider interposed between the Merchant and an Acquirer Member also complies with these Technical, Operational and Security Rules.

Members must have in place procedures that involve the application of reasonable care and diligence so as to satisfy themselves as to the integrity, solvency and reliability of third party Service Providers engaged in processing eftpos Transactions and/or undertaking activities as part of the eftpos Payment System on behalf of the Member., as well as owners of third party networks/devices. Checks to be carried out on third party Service Providers at the time of engagement and through the term of the service provision include, but are not limited to:

a. Credit check and/or other background investigations of the business and principal owners or officers of the business, when the information in the credit check is incomplete; and

b. Inspection of the premises to verify that the prospective Service Provider has the proper facilities, equipment, inventory and, where necessary, a license or permit to conduct the business; and

c. Documentary evidence of compliance with PCI DSS.

2.11. Business Continuity and Crisis Communication Plan

The Crisis Communication Plan and Member Incident Plan contained in the Australian Payments Network's Guidelines for IAC Participants contains guidance as to the possible crisis management corrective action that eftpos Issuers or eftpos Acquirers may need to take in the event of an unscheduled service disruption, fraudulent event or exposure.

Each Direct Connector and Direct Settler must maintain and test a business continuity and disaster recovery plan for its Direct Connection and Settlement arrangements (respectively) to demonstrate its ability to continue to meet requirements for the Direct Connection and Settlement arrangements (respectively) to be Available in the event of a Disabling Event, business interruption or a disaster being declared under the Direct Connector's business continuity and disaster recovery plan. If a Direct Connector or Direct Settler invokes its disaster recovery plan, it must immediately notify the Company that the plan is invoked.

If a Disabling Event or business interruption or a disaster suffered by a Direct Connector or Direct Settler relates to its host systems, its own business continuity and disaster recovery plan applies.

If a Disabling Event or business interruption or a disaster suffered by a Direct Connector relates to its Direct Connection to the eftpos Hub, then the Direct Connector must comply with the COIN Operating Manual in addition to its own business continuity and disaster recovery plan applies.

Direct Connectors to the eftpos Hub through a Standard Hub Service must comply with the COIN Operating Manual in respect of contingency.

Direct Connectors to the eftpos Secure Directory Server must comply with the business continuity and disaster recovery plan set out within the eftpos Secure Service Schedule.

Direct Connectors to the eftpos API Gateway must comply with the business continuity and disaster recovery plan set out within the eftpos API Gateway Service Schedule.

2.12. Fallback processing

Fallback is an important component of the eftpos Payment System which ensures that Cardholders and Merchants are able to complete legitimate eftpos Transactions in situations where normal online processing has been disrupted. Fallback is available to Acquirers / Merchants only as permitted in these Technical, Operational and Security Rules and any Fallback transactions not processed in accordance with these rules may be subject to a Disputed Transaction being raised by the Issuer (refer section 7). It is also important that Issuers do not indiscriminately raise a Disputed Transaction for Fallback transactions and that Acquirers ensure that Fallback transactions they process from Merchants are bona fide Fallback transactions.

2.12.1 Valid Fallback Transactions

Fallback transactions are prepared by the Merchant, in accordance with the provisions of these Technical, Operational and Security Rules, when the operator is unable to process a transaction online in the circumstances outlined below.

The Acquirer must require the Merchant to report the failure of the Terminal to the Acquirer's Help Desk as soon as possible after such failure becomes known by the Merchant.

In situations where a transaction has been declined "Issuer Unavailable", any subsequent transactions must be initiated by tapping (contactless) docking (Chip contact) or swiping (mag stripe) each Cardholder's card to check if the interchange link has been reinstated.

In the case of a Terminal failure, the Merchant should process Transactions through another Terminal if one is available and functioning, however, notwithstanding the availability of other Terminals at the Merchant location, failure at the Terminal to which the card is presented constitutes a Fallback situation.

a. Fallback processing is to be utilised only in the following circumstances:

    i. The card is a valid eftpos Card (including Multi-Network Card); and

    ii. The Terminal is not operating as a result of a genuine technical fault; or

    iii. No response is received to a transaction resulting in the Terminal "timing out"; or

    iv. The Terminal displays a message from the Acquirer host that the Issuer system is unavailable; or

v. The Acquirer has instructed the Merchant to use Fallback procedures for that particular Transaction.

b. Fallback processing is not supported for the following channels:

i. Point of Sale for Contactless Transactions

ii. Card Not Present eftpos Transactions;

iii. eftpos Mobile;

iv. eQR and eQR Pass Through Wallet, (Note: that the rules for eQR have not been ratified and are not yet applicable to Members) and

v. All channels for Prepaid Cards issued under a unique BIN and identified as "Electronic use only".

For clarity, although Fallback processing is not supported for contactless Transactions, a Merchant may direct a Consumer to insert their card following an unsuccessful contactless Transaction This is not considered to be a type of Fallback, nor does it preclude the subsequent contact Transaction (if it cannot be processed online) being processed as a Chip Fallback transaction as described in 2.12.3.1. (For clarity Contactless -only Terminals are excluded).

To avoid doubt, this does not prevent Fallback processing for Prepaid Cards that are not identified as "electronic use only".

2.12.2 Invalid Fallback Transactions

The Acquirer must instruct the Merchant NOT to prepare or perform a Fallback Transaction when the Terminal message in response to a transaction indicates that the:

a. Card is damaged (either the chip or magnetic stripe);

b. Card is suspected of being a Lost / Stolen Card;

c. Card presented is not a valid eftpos Card;

d. Card has expired;

e. Card limit is exceeded;

f. PIN entered is invalid; or

g. Transaction is declined for ANY reason other than "Issuer Unavailable".

A Disputed Transaction for invalid Fallback transactions may be raised by the Issuer (refer section 7).

2.12.3 Fallback types

The type of Fallback permitted, and the associated floor limits are determined by a combination of the card capability, Terminal capability, the capability of the interchange link to pass chip data and the capability of the Member host applications to process or validate it. Acquirers must not allow Merchants to process a second Fallback method when a previous Fallback method has been unsuccessful for the same transaction e.g. If Chip Fallback returns a declined response, the Merchant cannot process the transaction as an Electronic Fallback transaction.

2.12.3.1 Chip Fallback

2.12.3.1.1 Description

This applies to contact transactions only. eftpos does not support Chip Fallback for contactless transactions.

Chip Fallback is a transaction where the authorisation is delegated to the Card's chip when the transaction is unable to be processed online. To complete a Chip Fallback transaction the end to end process including the card, Terminal, interchange links and host applications must be chip enabled or the cryptographic services are processed by a third party on behalf of the Issuer host where the Issuer Host is not enabled. Chip Fallback limits are set on the Card's chip as stipulated in the eftpos Card Application Personalisation Specification, not at the device. Terminal limits must be set such that they will always defer to the Chip Fallback Limits when a Chip Fallback transaction occurs.

2.12.3.1.2 Eligible cards

Chip Fallback can only be performed on ACe enabled cards used on eftpos Chip and Contactless enabled Terminals.

2.12.3.2 Technology Fallback

2.12.3.2.1 Description

Technology Fallback is a transaction processed online using a Card's magnetic stripe when a Terminalis unable to communicate with a Card's chip. The merchant's eftpos Terminal must be set to a minimum of 2 attempts to read the Chip before Technology Fallback is invoked. For clarity, it is optional for mPOS – SPoC Terminals to support Technology Fallback. The subsequent transaction must include F47 Faulty Card Read FCR tag, be processed online as a magnetic stripe transaction with PIN and approved by the Issuer.

2.12.3.2.2 Eligible cards

Technology Fallback is permissible on all ACe enabled cards.

2.12.3.3 Electronic Fallback

2.12.3.3.1 Description

Electronic Fallback is a method used to capture a Card's track 2 data or track 2 equivalent data to generate a 0220 fallback message when a mag stripe Card (or Multi-Network Card where either the card or Terminal are not ACe enabled) is unable to go online. The transaction is subject to limits stipulated in Section 2.12.4.2 and are set at the Terminal. Electronic Fallback uses a signature CVM. Electronic Fallback is not permitted when another Fallback method has failed.

mPOS-SPoC Electronic Fallback shall not be supported when Mag stripe Transactions are supported.

For clarity, SPoC transactions are online only.

2.12.3.3.2 Eligible cards

Electronic Fallback is only permissible where;

a. The card is a mag stripe only card;

b. The card is a Multi-Network card that does not carry the ACe application;

c. The card is a Multi-Network card that has the ACe application but it is not enabled; or

d. The Terminal is not eftpos Chip enabled

The eftpos Hub Link Specification sets out the requirements for Electronic Interchange Fallback transactions.

2.12.3.4 Manual key entry

Manual key entry is a method invoked when mag stripe only Cards are unable to be processed due to a faulty card reader or PIN pad. Manual key entry must not be used when:

a. there is another Terminal available;

b. the card read fail is due to a faulty/damaged Card; or

c. the Card is an eftpos ACe enabled Card

Manual key entry may be phased out in the near future.

2.12.4 Fallback limits

Floor limits applicable to Fallback processing are a balance between the need to provide reasonable Fallback processing in a downtime situation and the risks associated with Fallback processing for the Issuer. An Acquirer must advise each Merchant of the floor limit applicable to that merchant facility as well as the zero floor limit for any cash, combined purchase/cash, contactless, eftpos Digital Acceptance or eftpos Mobile Transactions.

2.12.4.1 Chip Fallback limits

The limits applicable to Chip Fallback transactions are set out in the eftpos Card Application Personalisation Specification.

2.12.4.2 Electronic Fallback limits

Electronic Fallback limits are set at the Terminal and are applied to magnetic stripe transactions where normal online processing has been disrupted. The Merchant must not process two or more transactions (split sales) to avoid authorisation of a transaction value that exceeds its floor limit. Issuers can raise a Disputed Transaction for Fallback transactions where the Merchant has engaged in split sales processing and the Issuer has suffered a financial loss as a consequence.

MCC	Description	Total Transaction Amount (not exceeding)
All Merchants	Cash/combined purchase/cash	$0
5411	Supermarkets only	$200
5541	Service Stations	$60
5921	Liquor Stores	$60
5441	Convenience stores	$60
4121	Taxis/Limousines	$60
All other MCCs		$100

Table 2: Electronic Fallback limits

2.12.5 Split sales

During downtime, the Merchant must be required not to process two or more transactions (split sales) to avoid Authorisation of a Transaction value that exceeds its floor limit. Issuers can raise a Disputed

Transaction for Fallback transactions where the Merchant has engaged in split sales processing (except when the transaction is part of Instalment Payment Solution).

Merchants are to be advised that any split sale processing undertaken by the Merchant to avoid obtaining authorisation for above floor limit transactions, provides the Issuer with the right to raise a Disputed Transaction. A Disputed Transaction may be raised for the value that cannot be recovered by the Issuer, for the split transactions above the floor limit if it were to be processed as a single transaction processed on a particular Card by that Merchant.

2.12.6 Authorisation of Fallback Transactions above the floor limit

2.12.6.1 Support for Authorisations

Unless the Acquirer has advised Merchants of alternative procedures, Merchants are to contact the Acquirer to seek authorisation for Fallback Transactions that exceed the floor limit. Issuers may, but are not required to, elect to support a help desk for the purposes of providing a Fallback authorisation function.

2.12.6.2 Authorisation process where supported

Should an Issuer support an authorisation help desk, the Acquirer is to contact the Issuer help desk by telephone and advise:

a. Card number;

b. Cardholder name (if recorded on the Card);

c. Merchant Name;

d. Account selection;

e. Any cash component of the Fallback Transaction; and

f. Total amount of the Fallback Transaction.

Issuers may elect to automatically accept or reject Fallback Transactions for amounts in excess of floor limits prescribed by the Company. Where an authorisation is granted by an Issuer, an authorisation number is to be provided to the Acquirer and must be recorded by the Merchant as part of the Fallback record.

2.12.6.3 Authorisation process where not supported

Where an Issuer does not support an authorisation help desk the Acquirer must not authorise the transaction above the Fallback limits, unless the Issuer has provided the Acquirer with a blanket approval, to an agreed transaction amount, or to authorise Fallback Transactions on the Issuers behalf.

2.12.6.4 Voucher preparation

In circumstances where Electronic Fallback is permitted and the Acquirer's Terminal supports it, this facility must be used by the Merchant for Electronic Fallback processing except in cases of Terminal failure. Cardholder verification must be by means of the Merchant confirming the Cardholder signature on the Terminal produced voucher to that on the Card signature panel. Acquirers must seek authorisation from the Issuer for any Transactions that exceed the Merchants Fallback limits.

2.12.6.5 Warning bulletins

The provision for warning bulletins (paper or electronic) for lost, stolen or stopped cards are not supported at eftpos.

2.12.6.6 Retention of records

The Merchant is to be advised by the Acquirer to retain the Merchant copy of signed electronic Fallback vouchers for a minimum of 12 months unless a longer period is specified by the Acquirer.

The Issuer is to maintain a suitable record of Fallback Authorisation requests received from Acquirers and the response (approved or declined) it has provided, however, it is optional for Issuers to verify Fallback Transactions it receives against this record.

2.12.7 Interchange Fallback specifications

For Direct Connectors to the eftpos Hub the interchange specification for Fallback messaging is in the eftpos Hub Link Specification.

2.12.8 Clearance of Interchange Fallback Transactions

The Acquirer must despatch Fallback Transactions to the Issuer as 0220/0221 Fallback Transaction messages (as specified in the eftpos Hub Link Specification for Direct Connections to the eftpos Hub) at the earliest opportunity and no more than 10 days after the Transaction date.

2.12.9 Acceptance of Interchange Fallback Transactions

The Issuer undertakes to accept a Fallback Transaction relating to Cards issued by it, provided:

a. a Financial Transaction Advice message has been prepared by the Acquirer in accordance with agreed procedures, and

b. the individual amount of the Fallback Transaction does not exceed the Merchant's Fallback Floor Limit set by the Company for magnetic stripe transactions or,

c. the Fallback Transaction does not exceed the cards Chip fallback limit, and

d. the Financial Transaction Advice Message contains a valid Authorisation number for Transactions in excess of the Merchant's Fallback Floor Limit, and

e. Fallback Transactions have been charged to the Issuer in the agreed manner, and

f. there is no evidence of split-transaction processing by the merchant (i.e. multiple transactions on the same card at the same merchant within a short period of time) or merchant complicity in fraudulent cardholder transactions.

2.12.10 Tracing of Fallback Transactions

The Acquirer is required to maintain suitable records to ensure the positive identification of Fallback Transactions as advised by the Issuer to enable the Transaction to be processed by the Issuer or to satisfy a query from the Cardholder. A copy of a Fallback record must be provided within 26 days of the date of the Issuer request.

2.13. Reports

This section applies in addition to Clause 9.

2.13.1 General

Each Issuer and Acquirer must ensure that all reports of eftpos Transactions that it is required to produce for the purposes of this section and Clause 9 contain information which:

a) satisfies its own internal audit requirements;

b) provides the ability to trace Items in the event of Transaction discrepancies/enquiries;

c) assists in verifying settlement figures;

d) provides statistical information at a level that enables the Member to meet its reporting obligations under the Scheme Rules; and

e) assists the Company to perform various governance and analytics activities, evaluate performance of the eftpos Scheme and Member compliance with the Scheme Rules and these Technical, Operational and Security Rules.

All eftpos Transactions processed through Interchange, both completed and uncompleted/declined, must be reported to assist with Cardholder and/or Merchant enquiries and reconciliation procedures.

2.13.2 Types of reports

Each Issuer and Acquirer in their own right and on behalf of their Direct Connector(s) must be capable of producing the following reports:

a. a daily listing of all eftpos Transactions which specifies:

   i. Cardholder Number (Field 02) (with truncated card numbers to comply with PCI DSS)

   ii. Transaction type and account type selected (from Field 03 – Processing Code)

   iii. Transaction Amount (Field 04) plus any Cash Out value (Field 57)

   iv. Acquirer date and time stamp of the Transaction (Field 07)

   v. Acquirer Reference Number (STAN - Field 11 or RRN - Field 37)

   vi. Acquirer's Transaction Settlement Date (Field 15)

   vii. POS Entry Mode (Field 22)

   viii. PAN Sequence Number (Field 23) for Chip read or eftpos Mobile transactions

   ix. Issuer Sequence Number (if used) for mag stripe transactions

   x. Acquiring Institution Identification Code (Field 32)

   xi. Authorisation Response Code (Field 39 of Response Message)

   xii. Terminal Identification Number (Field 41)

   xiii. All tags in Field 47

   xiv. Field 55

b. a daily Member Batch File;

c. a Member Monthly Report as required for the purposes of section 9;

d. Monthly Member interchange reporting for the purposes of section 9; and

e. No longer used.

Each Member, on behalf of their Direct Connector(s) using the eftpos API Gateway must be capable of producing the following reports:

a. Gateway batch file reports

2.13.3 Retention period

Reports produced by each Member under 2.13.2 (b), (c) (d) and (e) are to be held for a minimum period of 12 months in such a manner that they are capable of being retrieved or reproduced within 10 business days. Reports produced by each Member under 2.13.2 (a) are to be held for a minimum period of 30 days. Longer retention periods may be required by legislation; industry regulator(s) or the Member's own policies.

2.14. Enquiries

2.14.1 Disputed Transactions

The Company will maintain a contact list for each Member.

Clause 7 sets out the requirements for Disputed Transactions and Chargebacks. eftpos Disputes and Chargebacks support arrangements and Company contacts are detailed in the eftpos Disputes and Chargebacks Service Member Operations Guide as issued by the Company from time to time.

2.14.2 Settlement enquiries

The Company will maintain a contact list for each Direct Settler.

For Direct Connections to the eftpos Hub, refer to the Standard Hub Service Schedule for settlement and reconciliation support services. eftpos Settlement support arrangements and Company contacts are detailed in the eftpos Settlement Service Member Operations Guide as issued by the Company from time to time.

For Members that settle bilaterally, any enquiries regarding bilateral Settlement and any related discrepancies are to be directed to the appropriate counterparty contact. Each Member that settles bilaterally must maintain and provide up to date and accurate contact details to each other Member with whom they settle bilaterally.

2.14.3 System operational enquiries/advices

For Direct Connections to the eftpos Hub, refer to the Standard Hub Service Schedule for fault rectification and escalation procedures. For Direct Connections to the eftpos Hub, all problems resulting in unscheduled downtime and general enquiries regarding Interchange Link problems are to be directed to the number published by the Company to Members for assistance enquiries.

For Direct Connections to the eftpos TSP, refer to the eftpos Mobile Service Schedule and eTS-F Service Schedule for fault rectification and escalation procedures.

For Direct Connections to eftpos Secure Directory Server, refer to the eftpos Secure Services Schedule for fault rectification and escalation procedures.

For Direct Connections using the API Gateway, refer to the eftpos API Gateway Services Schedule for fault rectification and escalation procedures.

2.14.4 Escalation procedures for unscheduled outages

For Direct Connections to the eftpos Hub, refer to the Standard Hub Service Schedule for fault rectification and escalation procedures.

For Direct Connections to the eftpos TSP, refer to the eftpos Mobile Service Schedule and eTS-F Service Schedule for fault rectification and escalation procedures.

For Direct Connections to eftpos Secure Directory Server, refer to the eftpos Secure Services Schedule for fault rectification and escalation procedures.

For Direct Connections using the eftpos API Gateway, refer to the eftpos API Gateway Services schedule for fault rectification and escalation procedures.

2.15. Fees

Fees applicable to eftpos Transactions between Members, and fees payable to the Company, are set from time to time by the Company pursuant to the Scheme Rules.

The requirements relating to the payment of fees (due to or due by the Member) are specified in the Scheme Rules.

Fees applicable to eftpos Secure service calls between Members, Direct Connectors and the Company, and fees payable to the Company, are set from time to time by the Company pursuant to the Scheme Rules.

3. Issuer Standards

3.1. Test tools

3.1.1 Production of test cards

Issuers are required to provide Acquirer Members and the Company with an appropriate number of test cards in sufficient time to enable testing to occur for any new BINs to be introduced by the Issuer or any change of BIN routing requested by the Issuer.

The Company may produce and provide, to a Member, test eftpos Form Factors for Acceptance Devices and, to a Direct Connector, test eftpos Form Factors for Direct Connection testing and certification. Any test eftpos Form Factors provided by the Company are provided “as is”, for the sole use of the Member or the Direct Connector as the case may be and must not be provided by the Member or Direct Connector to any other person. The Company has no liability in respect of any test eftpos Form Factors provided by the Company.

3.1.1.1 eftpos Hub

The testing protocol for Direct Connections to the eftpos Hub including support for Payment Token data is set out in the Standard Hub Service Schedule.

3.1.1.2 eftpos Chip and Contactless

Provision of test tools for eftpos Chip and Contactless certification are detailed in the respective eftpos Certification Body procedure documents.

3.1.1.3 eftpos Mobile

Participating Issuers will be notified of the certification requirements by the eftpos Certification Body for implementation of eftpos Mobile as part of a Cloud Based Payment Solution. Test tools for eftpos Mobile are detailed in the eftpos CBP Solution Interoperability Testing Requirements.

Test tools and certification requirements for eftpos Mobile using OEM Solutions are set out in the eftpos Mobile Implementation Guide related to the relevant OEM Solution.

3.1.1.4 eftpos Secure

Participating Members and Direct Connectors will be notified of the certification requirements by the eftpos Certification Body for implementation of eftpos Secure. Test tools, processes and requirements for eftpos Secure are set out in the eftpos Secure Implementation Guide.

3.2. Characteristics of eftpos Cards

3.2.1 Physical characteristics of Cards

Each Issuer must ensure that the Cards that it issues for use in the eftpos system, comply with the specifications detailed in; AS 3522, AS 3524 and ISO 7816. These standards detail the requirements for the physical Card characteristics (including dimensions and layout of the card chip, contactless antennae and Card personalisation), information relating to the data elements for Chips and the encoding format for Tracks 1 and 2 of the magnetic stripe.

Issuers must also ensure that word “debit” is displayed on the front of all the eftpos Debit cards issued after 1 November 2019.

3.2.2 Minimum personalisation requirements for Cards

The layout of Card brand marks and personalisation are detailed in the eftpos Brand and Style Guide.

3.2.2.1 Card information personalisation

Issuers must ensure that eftpos cards issued for use in the eftpos system are personalised with the following information, as a minimum:

a. Card/account number (PAN); and

b. Card expiry date

This data must match the detail encoded in Track 2 on the magnetic stripe as it is utilised in Fallback processing.

It is recommended that the Cardholder name is also recorded on the Card. Any other information recorded on Cards by the Issuer must be in accordance with the specifications detailed in AS 3522.

eftpos Cards must be able to be identified visually and electronically as being debit Cards.

3.2.2.2 Card expiry

The card expiry date must be clearly recorded on the card and must identify the month and the year of the card expiry. It is recommended that the card artwork includes printing below the recorded date to unambiguously identify the format of the card expiry date, e.g. Month / Year, MM/YY.

The Card will be deemed to expire on the first day of the subsequent month following the date specified in the recorded card expiry date.

The validity period of the card is at the Issuer's discretion. It is recommended that the Card be issued with a validity period of no more than four (4) years.

3.2.2.3 Card printing requirements

Personalisation for eftpos (proprietary) Chip and Dual interface Cards may be applied using flat graphics/thermal printing or embossing. It is recommended that a top coat is also applied to ensure durability of information recorded in this manner.

3.2.3 Minimum personalisation requirements for Chip Cards

Issuers must ensure that the chip on Cards issued for use in the eftpos Payment System are personalised in accordance with the eftpos Card Application Personalisation Specification.

3.2.3.1 Integrated Chip Card life

The life of an Integrated Chip Card product cannot extend beyond 15 years from the date of certification of the Card's chip. Renewal of eftpos certification will occur at intervals during this timeframe, where appropriate, in accordance with the eftpos Certification Body documentation. All cards must be removed by this time.

3.2.4 Card personalisation – Keys [Clause 3.2.4 is confidential]

3.2.5 Encoding requirements for eftpos Cards

Where a magnetic stripe is applied, encoding of Track 2 is mandatory and must be in accordance with AS 3524. The encoding of other Tracks on the magnetic stripe is optional, however, if Track 1 is encoded it must also be in accordance with AS 3524.

3.2.6 Minimum signature panel requirements

A signature panel is optional on eftpos Cards. Where it is applied, the signature panel must comply with the following minimum standards.

The minimum size standards for the signature panel are:

a. Minimum width (length) to be 45.00 mm;

b. Maximum width to be 57mm for chip cards and

c. Minimum height to be 8.00 mm.

The position of the signature panel on the reverse of the card must not interfere with the Chip or magnetic stripe and must not intrude into the embossed area of the Card. Where a card does not contain a chip and there is a signature panel present, the signature panel may run the full width of the Card.

3.2.6.1 Minimum signature panel requirements – security pattern

The signature panel applied may incorporate the eftpos security pattern on the face of the panel as specified in the eftpos Card branding and contactless requirements style guide.

It is also recommended that a repetitive “VOID” pattern is printed on the plastic core in the area covered by the signature panel.

3.2.7 eftpos Consumer Identification, Verification and Authentication for eftpos Cards

Issuers are required to:

a. perform identification and verification, as required by Law, when a relationship is initiated with an eftpos Consumer;

b. authenticate an eftpos Consumer during an eftpos Transaction, excluding eftpos Transactions below Issuer defined CVM limits or where a Transaction with No CVM is permitted (unless otherwise stated in these Technical, Operational and Security Rules for an eftpos Form Factor, this can be through use of a PIN or any other method approved by the Company); and

c. authenticate an eftpos Consumer at any point in the relationship between the Issuer and the eftpos Consumer where the Issuer:

   i. has a requirement outside those of the eftpos Payment System to authenticate an eftpos Consumer; or

   ii. makes a determination that identification and verification or authentication of an eftpos Consumer is required.

The method of identification, verification or authentication of an eftpos Consumer, other than verification performed as part of an eftpos Transaction, is determined by the Issuer.

3.3. Characteristics of eftpos Prepaid Cards

Prepaid Program Providers and sponsoring Issuers must ensure that Prepaid Cards comply with the following requirements.

3.3.1 Physical characterisitcs of eftpos Prepaid Cards

Prepaid Cards must as a minimum, meet the specifications detailed in AS 3521, AS 3522 and AS 3524. These standards contain requirements for physical characteristics, dimensions, layout of information and format for encoding Tracks 1 and 2 of the magnetic stripe.

(Note: Cards that do not comply with these requirements may not be able to generate Transactions at eftpos Terminals.)

3.3.2 Minimum perosnalisation requirements for eftpos Prepaid cards

3.3.2.1 Prepaid Card information personalisation

There are no mandatory requirements for the personalisation of eftpos Prepaid Cards outside the requirements for eftpos Prepaid Cards and associated collateral stipulated in the eftpos Brand and Style Guide.

eftpos Prepaid Cards must be identified as such by:

a. having the word "Prepaid" or "Gift card" clearly printed on the face of the card; To use the word "Gift card" on the face of the card, the word "Prepaid" must remain on the back of the card and, where applicable

b. indicating that they can only be used when online authorisation is available by having the words "Electronic use only" or similar printed on the card.

eftpos Prepaid Cards must be identified as being Prepaid Cards using the methods above and must be capable of being electronically identified as Prepaid cards. The recording of the PAN and expiry date on eftpos Prepaid Cards is optional.

3.3.2.2 Card expiry

eftpos Prepaid Cards must be issued for a minimum expiration period as required by the Law.

The Card will be deemed to expire on the first day of the subsequent month following the date specified as the card expiry date.

3.3.2.3 Encoding requirements for eftpos Prepaid Cards

Prepaid Cards are to have Track 2 encoding in accordance with the requirements of AS 3524.

Acquirers are required to transmit all Track 2 data captured at the Terminal to the Issuer without alteration.

3.3.2.4 Minimum signature panel requirements

There is no mandatory requirement for a signature panel on Prepaid Cards.

3.3.3 PIN standards

The use of a Cardholder Verification Method (CVM) or other method for cardholder authentication is mandatory for reloadable Prepaid Cards with ACe. Offline enciphered PIN shall not be supported for reloadable Prepaid Cards with ACe.

The use of a PIN or other method for cardholder authentication is not mandatory for Prepaid Cards that do not have eftpos chip application (no ACe). However, when prompted to enter a PIN at the Terminal, the entry of a four digit number is mandatory to facilitate the carriage of the Transaction across the eftpos Payment System.

3.3.4 eftpos Consumer Identification and Verification for eftpos Prepaid Cards

Subject to any Law that applies to Prepaid Card issuance, identification and verification of eftpos Consumers using an eftpos Prepaid Card is mandatory as applicable and is determined by the Card Issuer.

3.3.5 Disputes

Where a Prepaid Card is issued subject to transactions being initiated with a CDCVM or PIN issued to the original Cardholder (the security of which is managed in compliance with clause 3.7.1.1 of these Rules) then the eftpos Disputed Transactions process defined in Section 7 will apply.

Where a Prepaid Card is issued without a PIN or where the PIN does not meet the security requirements in Annexure A to volume 2 of the IAC Code Set, then cardholder disputes relating to electronically processed transactions are to be resolved by the Prepaid Program Provider or the Issuer without reference to the Acquirer.

3.3.6 Medicare claim refunds

Medicare claim refunds must not be processed to a Prepaid card.

3.4. Characteristics of eftpos Mobile

There are 5 concepts that may be relevant to eftpos Mobile, depending on the solution used. Those concepts are set out below as an overview.

a. **Token Requestor registration** – a Token Requestor wishing to be able to request Payment Tokens to be assigned to a Mobile Device for eftpos Mobile must register with the Company and receive a Token Requestor ID. Members wishing to use a third party Token Requestor must register the Token Requestor with the Company. The Token Requestor ID must be provided as part of any Provisioning or Payment Token lifecycle event request sent to the Company.

b. **eftpos Consumer and account authentication** – this involves the eftpos Issuer performing:

   i. Identification and Verification (ID&V) of the eftpos Consumer; and

   ii. a check of the account for validity.

c. **Provisioning** – this is the generation of a Payment Token (which can be performed by either the Mobile Wallet Provider or the Company depending on the solution), personalisation of the Payment Token for the Mobile Device and delivery of the Payment Token and other specified information (see clause 5.7) to the Mobile Device. Payment Token generation can be done by the Company as Token Service Provider (TSP) or by the Issuer or its third party service provider as TSP via the Company as Trusted Service Manager (TSM). In the case of OEM Solutions, the Company, as TSM, will only accept Payment Token Provisioning requests from registered Token Requestors.

d. **Token Lifecycle Management (performed by a TSM)** – this is the initial mapping of the Payment Token to the PAN and setting or changing the status of the Payment Token according to lifecycle events (see clause 5.7). Where the Company is the TSM, it will manage Payment Tokens according to instructions that may be received from Mobile Wallet Providers or registered Token Requestors (as relevant to the solution).

e. **Payment processing using Payment Tokens** – this is the processing of a payment initiated using a Payment Token assigned to the Mobile Device when used at an ACe enabled eftpos Terminal and routed by the Acquirer according to the Token BIN. When received at the eftpos Hub, the transaction will either be:

   i. de-tokenised and sent to the Issuer, where the Company is the TSP; or

   ii. sent to the Issuer for De-Tokenisation and processing, where the Issuer is the TSP.

The eftpos Hub Link Specification and relevant eLS Addendums sets out the messages exchanged to achieve these processes for the relevant OEM Solution. The eftpos API Interface Specification sets out the messages exchanged to achieve these processed for Direct Connections to the eftpos TSP.

3.4.1 Solution options and requirements for eftpos Mobile

eftpos Transactions supported for eftpos Mobile may be initiated by a Mobile Device capable of accessing an eftpos Account using any of the following methods, each in accordance with the pre-requisites in clause 3.4.1.2 and minimum requirements in clause 3.4.1.3:

a. a Cloud Based Payments Solution (CBP Solution) in a Mobile Wallet that meets the requirements of these Technical, Operational and Security Rules; or

b. an OEM Solution.

Each of the above is considered to be, without limitation, examples of an eftpos Form Factor for the purposes of eftpos Mobile and the eftpos Scheme Rules and each relies on the use of a Payment Token (see clauses 3.4.8 and 5.7).

The Company will notify Members when an eftpos applet which enables eftpos Cards and/or eftpos Accounts to be Provisioned for eftpos Mobile has been embedded into Mobile Devices manufactured by Original Equipment Manufacturers (OEMs).

For clarity, provisioning may occur for eftpos Mobile whether or not a physical eftpos Card has been issued in relation to that eftpos Account. At a minimum, where there is no physical Card, or are physical Card is a Multi-Network Card, a virtual eftpos card number is required to be generated and linked to the eftpos Account. Refer to the eftpos Mobile Member Implementation Guide and eftpos Brand and Style Guide for the relevant eftpos Mobile solution requirements related to the provisioning of an eftpos Account for eftpos Mobile.

3.4.1.1 No longer used

3.4.1.2 Pre-requisites for eftpos Mobile

This clause sets out the pre-requisites to enable a Mobile Device for eftpos Mobile.

3.4.1.2.1 Cloud Based Payment Solutions

There are two CBP Solutions available for eftpos Mobile:

a. Issuer Wallet; or

b. Open Wallet.

A Mobile Device to be used for eftpos Mobile through a CBP Solution can use any operating system that supports mobile payments with a near field communications controller.

For clarity, eftpos Cards to be digitised as part of eftpos Mobile are not required to be eftpos Chip and Contactless enabled.

3.4.1.2.1.1 Issuer Wallet

In the case of eftpos Issuers enabling an Issuer Wallet, where the Issuer has elected to Provision eftpos Mobile, the eftpos Issuer must:

a. have a direct or indirect connection to the eftpos Hub;

b. where the eftpos Issuer has appointed a Token Requestor, have a Direct Connection between the Token Requestor and the eftpos TSP;

c. where the eftpos Issuer is not a Member, be sponsored by a Member which remains responsible for the compliance by the eftpos Issuer with these Technical, Operational and Security Rules;

d. do each of the following:

   i. in the case of Multi-Network Cards, digitise an eftpos Account and display or cause to be displayed a representation of each eftpos Account (whether as a photo of an issued Card, virtual Card or otherwise) in the Issuer Wallet in accordance with the eftpos Mobile Member

Implementation Guide for the relevant eftpos Mobile solution and the eftpos Brand and Style Guide; or

ii. in the case of proprietary Cards, either digitise an eftpos Account in accordance with sub-clause (i) above or digitise the eftpos Card; and

iii. in each case assign or cause to be assigned a Payment Token, unique for use in the Issuer Wallet for the purposes of the eftpos Payment System, with:

A. a PIN or other authentication method approved by the Company for each Card being digitised (where a Card is digitised) being mapped back to the relevant eftpos Account to which the Card is mapped for debit payments; or

B. a PIN or other authentication method approved by the Company being issued for each eftpos Account (where a Card is not digitised) that is Provisioned;

e. have the ability to suspend any one or more payment methods that may be available within the Mobile Wallet without restricting access to the Mobile Wallet; and

f. include:

i. in the case of proprietary Cards, an eftpos AID linked to an eftpos Account being digitised in the Issuer Wallet;

ii. in the case of Multi-Network Card, either the eftpos Savings AID or eftpos Cheque AID for each eftpos Account being digitised in the Issuer Wallet; and

iii. in all other cases, an eftpos AID relevant to at least one eftpos Account being digitised in the Issuer Wallet.

3.4.1.2.1.2 Open Wallet

In the case of an Open Wallet, where the Issuer has elected to Provision eftpos Mobile, providers must:

a. have a direct or indirect connection to the eftpos Hub;

b. where the Issuer has appointed a Token Requestor, have a Direct Connection between the Token Requestor and the eftpos TSP;

c. where the provider is a third party non-Member, be sponsored by a Member which remains responsible for the compliance by the provider with these Technical, Operational and Security Rules;

d. display or cause to be displayed a representation of the eftpos Account (whether as a virtual Card or otherwise) enabled for use in the Open Wallet in accordance with the eftpos Mobile Member Implementation Guide for the relevant eftpos Mobile solution and the eftpos Brand and Style Guide;

e. assign or cause to be assigned a Payment Token, unique for use in the Open Wallet for the purposes of the eftpos Payment System, together with one PIN or other authentication method approved by the Company for use with that Payment Token for that Mobile Wallet;

f. have the ability to suspend any one or more payment methods that may be available within the Mobile Wallet without restricting access to the Mobile Wallet;

g. as a single Payment Token is issued for all payment methods within a Mobile Wallet, ensure that each payment method has an identifier in the transaction message to uniquely identify the payment method being used (using the Card Sequence Number); and

h. include an eftpos AID in the Mobile Wallet.

3.4.1.2.2 OEM solutions

In the case of an OEM Solution, the eftpos Issuer must:

a. have a direct or indirect connection to the eftpos Hub;

b. where the eftpos Issuer has appointed a Token Requestor, have a Direct Connection between the Token Requestor and the eftpos TSP;

c. where the eftpos Issuer is not a Member, be sponsored by a Member which remains responsible for the compliance by the eftpos Issuer with these Technical, Operational and Security Rules;

d. do each of the following:

   i. in the case of Multi-Network Cards, digitise an eftpos Account and display or cause to be displayed a representation of each eftpos Account (whether as a photo of an issued Card, virtual Card or otherwise) in the Issuer Wallet in accordance with the eftpos Mobile Member Implementation Guide for the relevant eftpos Mobile solution and the eftpos Brand and Style Guide;

   ii. in the case of proprietary Cards, either digitise an eftpos Account in accordance with sub-clause (i) above or digitise the eftpos Card; and

   iii. in each case assign or cause to be assigned a Payment Token, unique for use in the Issuer Wallet for the purposes of the eftpos Payment System, with:

      A. a PIN or other authentication method approved by the Company for each Card being digitised (where a Card is digitised) being mapped back to the relevant eftpos Account to which the Card is mapped for debit payments; or

      B. a PIN or other authentication method approved by the Company being issued for each eftpos Account (where a Card is not digitised) that is Provisioned.

For clarity, eftpos Cards to be digitised as part of eftpos Mobile are not required to be eftpos Chip and Contactless enabled.

3.4.1.3 Minimum requirements for eftpos Mobile

3.4.1.3.1 Minimum requirements of a Mobile Wallet for Cloud Based Payment Solutions

A Mobile Wallet through a Cloud Based Payments Solution to which an eftpos Form Factor is enabled as part of eftpos Mobile must, at a minimum:

a. comply with the eftpos Cloud Based Payments Solution Technical Recommendations as issued by the Company from time to time;

b. comply with the eftpos Mobile Applet Personalisation Specification as issued by the Company as issued from time to time;

c. provide an eftpos Consumer:

   i. in the case of an Issuer Wallet - access to all eftpos AID options applicable to the Card or eftpos Account being enabled must be present; or

   ii. in the case of an Open Wallet - access to at least one of the eftpos Savings and eftpos Cheque AIDs;

d. No longer used.

e. where the Mobile Wallet offers functionality for an eftpos Consumer to select their preferred account or network, ensure that each eftpos Consumer has the ability to set and change the default or priority payment selection at the time of enablement and at any time afterwards, so that any available eftpos AID can be selected as the eftpos Consumer's default or primary payment choice on a per transaction or account settings basis;

f. assign or cause to be assigned a Payment Token, unique to use of the Mobile Wallet for the purposes of the eftpos Payment System, in accordance with the BIN requirements in clause 3.9, with the PIN or other authentication method approved by the Company:

   i. In the case of an Issuer Wallet - for each Card and eftpos Account being digitised being mapped back to the relevant eftpos Account to which the Card or eftpos Account is mapped;

   ii. In the case of an Open Wallet - for use with that Payment Token and which is not used in conjunction with any issued Card or eftpos Account;

g. provide for the remote removal of static and dynamic data by the Mobile Wallet Provider at the request of the eftpos Consumer;

h. the Mobile Wallet must facilitate disablement after periods of inactivity in accordance with perimeters set by the Mobile Wallet Provider; or

i. not require the eftpos Consumer to tap more than once for a single transaction.

Use of a Mobile Wallet must not breach any of the requirements relating to accounts accessible using the Mobile Wallet, such as Merchant or channel based restrictions. Where the Mobile Wallet Provider is not the Issuer of the original payment method, the Mobile Wallet Provider is required to pass relevant data elements in the transaction message to the Issuer of the original payment method, to allow a decision to be made by that Issuer during transaction processing. Further details are included within the eftpos Cloud Based Payments Solution Technical Recommendations.

3.4.1.3.2 Minimum requirements for eftpos Mobile using an OEM Solution

A Card and/or an eftpos Account may be enabled for eftpos Mobile using an OEM Solution at the request of an OEM where the eftpos Issuer has notified the Company that it has permitted its Cards and/or eftpos Accounts to be Provisioned into the Mobile Device for the purposes of the eftpos Payment System. eftpos Issuers must or cause an OEM in an OEM Solution to, at a minimum:

a. be registered as a Token Requestor and have been assigned a Token Requestor ID by the Company;

b. risk assess eftpos Payment Token provisioning requests and support eftpos Consumer ID&V;

c. perform Card and eftpos Account authentication;

d. comply with any eftpos Mobile Member Implementation Guide that applies to OEM Solutions;

e. comply with the eftpos Mobile Applet Personalisation Specification as issued by the Company from time to time;

f. provide an eftpos Consumer, access to all eftpos Cards (in the case of proprietary cards) and eftpos Accounts (in the case of Multi-Network Cards & Proprietary Cards) issued by the eftpos Issuer to that eftpos Consumer;

g. No longer used.

h. where the Mobile Wallet offers functionality for an eftpos Consumer to select their preferred network or account, ensure that each eftpos Consumer has the ability to set and change the default or priority payment selection at the time of enablement and at any time afterwards, so that any available eftpos Account selection can be selected as the eftpos Consumer's default or primary payment choice on a per transaction or account settings basis;

i. assign or cause to be assigned a Payment Token, unique to use for the purposes of the eftpos Payment System, in accordance with the BIN requirements in clause 3.9, with:

    i. a PIN or other authentication method approved by the Company for each Card being digitised (where a Card is digitised) being mapped back to the relevant eftpos Account to which the Card is mapped for debit payments; or

    ii. a PIN or other authentication method approved by the Company being issued for each eftpos Account (where a Card is not digitised) that is Provisioned; and

j. exchange communications relating to lifecycle events

3.4.2 Physical characteristics of eftpos Mobile

An eftpos Form Factor enabled for eftpos Mobile must meet the requirements set out in these Technical, Operational and Security Rules and the eftpos Brand and Style Guide.

Additional guidance regarding the physical characteristics of an eftpos Form Factor enabled for eftpos Mobile is set out in the relevant eftpos Mobile Member Implementation Guide including the eftpos user experience recommendations.

The full PAN must not be displayed as part of the user display on the Mobile Device to which an eftpos Form Factor is Provisioned unless the eftpos Consumer has unlocked their application in the Mobile Wallet. The use of a Masked PAN where either the first 6 and last 4 digits or just the last 4 digits of a PAN are displayed is permitted.

3.4.3 Minimum personalisation requirements for eftpos Mobile

3.4.3.1 Information personalisation for eftpos Mobile using a CBP Solution

eftpos Form Factors enabled for use with eftpos Mobile using a CBP Solution must be personalised in accordance with the eftpos Mobile Applet Personalisation Specification as published by the Company from time to time.

Conformance with the requirements detailed in the eftpos Mobile Applet Personalisation Specification is evidenced through the eftpos Cloud Based Payments Solution Interoperability Test Requirements, and associated implementation checklists issued by the Company from time to time.

3.4.3.2 Information personalisation for eftpos Mobile using an OEM Solution

eftpos Form Factors enabled for use with eftpos Mobile using an OEM Solution must be personalised in accordance with the eftpos Mobile Applet Personalisation Specification as published by the Company from time to time.

3.4.3.3 Expiry of Form Factors enabled for eftpos Mobile

The validity period of the eftpos Form Factor created by enabling an eftpos Account for eftpos Mobile is at the Mobile Wallet Provider's discretion, up to a maximum expiry period of 20 years.

Where an eftpos Account as represented by a Card has been enabled for eftpos Mobile, the expiry date of the Payment Token will be replaced with the expiry date of the Card at the time of De-Tokenisation.

See clause 5.7 for expiry dates related to Payment Tokens.

3.4.4 Personalisation – Keys [Clause 3.4.4 is confidential]

3.4.5 eftpos Consumer Identification and Verification methods for eftpos Mobile

The method of Identification and Verification (ID&V) of an eftpos Consumer to use eftpos Mobile is dependent on the eftpos Mobile solution offered and utilised by the eftpos Consumer.

Where:

a. an eftpos Form Factor is to be enabled for eftpos Mobile in a Cloud Based Payments Solution, the method of ID&V is determined by the Mobile Wallet Provider, based on the risk management requirements of a Mobile Wallet Provider and in accordance with applicable Laws; and

b. an eftpos Form Factor is to be enabled for eftpos Mobile through an OEM Solution the ID&V methods selected by the eftpos Issuer must comprise at a minimum, one mandatory method and one optional method detailed in the eftpos Mobile Member Implementation Guide for the relevant OEM Solution and otherwise in accordance with applicable Laws.

3.4.5.1 Prohibited eftpos Consumer Identification and Verification methods for eftpos Mobile

Mobile Wallet Providers are not permitted to verify the identity of the eftpos Consumer for eftpos Mobile using any of the following methods:

a. verification through the use of the PIN issued with the eftpos Form Factor;

b. verification through a second use of a temporary password provided by the Mobile Wallet Provider or eftpos Issuer (as the case may be) which has not been changed by the eftpos Consumer;

c. static authentication data, except that secret questions are permitted; or

d. enrolment in an online authentication service at the time of eftpos Consumer verification.

If the Company is the TSM, the eftpos Issuer will notify the Company, where an eftpos Consumer fails the ID&V method used.

eftpos Mobile must not be made available to an eftpos Consumer, where no verification of the eftpos Consumer has been completed.

3.4.5.2 When eftpos Consumer Identification and Verification is required

3.4.5.2.1 CBP Solutions

Mobile Wallet Providers must perform a form of:

a. Identification and Verification of the eftpos Consumer at the time an eftpos Form Factor is enabled for eftpos Mobile as part of a Mobile Wallet; and

b. authentication of the eftpos Consumer:

   i. if the Mobile Wallet is configured by the eftpos Consumer to require:

      A. the Mobile Device to be unlocked for use; or

      B. the Mobile Wallet application to be unlocked for each use; and

   ii. at the time of providing a direction to resume a Payment Token, based on criteria set by the Mobile Wallet Provider

3.4.5.2.2 OEM Solutions

eftpos Issuers must perform a form of:

a. Identification and Verification of the eftpos Consumer at the time a Card Provisioning is requested for eftpos Mobile using an OEM Solution; and

b. Authentication of the eftpos Consumer:

   i. if the eftpos Consumer configures the Mobile Device to require:

      A. the Mobile Device to be unlocked for use; or

      B. the OEM Solution payment application to be unlocked for each use; and

   ii. at the time of providing a direction to resume a Payment Token, based on criteria set by the Mobile Wallet Provider

3.4.6 Security requirements for offering eftpos Mobile

Any Mobile Wallet Provider who enables an eftpos Form Factor to be used for eftpos Mobile in a Mobile Wallet must comply with the requirements set out in the eftpos Cloud Based Payments Solution Technical Recommendations as issued by the Company from time to time.

An eftpos Issuer that enables eftpos Mobile using an OEM Solution must comply with clause 3.4.1.3.2.

3.4.7 No minimum qualification criteria for eftpos Consumers

There are no minimum qualification criteria for eftpos Consumers to participate in eftpos Mobile, although a compatible Mobile Device and at least intermittent internet connectivity are required.

3.4.8 Provisioning of an eftpos Form Factor on a Mobile Device [Clause 3.4.8 is confidential]

3.5. Use of brand marks

All eftpos Form Factors must comply with the eftpos Brand and Style Guide.

All proprietary eftpos Cards must have the eftpos Logo on the front of the Card. All proprietary eftpos Cards used or displayed for eftpos Digital and eftpos Mobile must have the eftpos Logo as a cobrand logo on the part of the design that is viewable on the payment selection page display or in a mobile wallet where the payment selection page or wallet carries multiple representations of cards.

All eftpos Cobrand Cards must have the eftpos Logo on the front of the Card. The eftpos logo may co-reside with other payment scheme marks as prescribed in the eftpos brand guide and style guide.

For clarity, all Multi-Network Cards associated with form factors used for eftpos Mobile must have the underlying eftpos Account Provisioned for eftpos Mobile and:

a. have the eftpos Logo on the front of the virtual Card or visual representation of the Card as a separate visual representation of the Card from any representation of any other functionality available using the Multi-Network Card;

b. have the eftpos Logo on the part of the design that is viewable on the payment selection page display or in a mobile wallet where the wallet carries multiple representations of cards; and

c. provide equal prominence for the eftpos Logo on any Card or form factor visual representation of the Card or payment selection page that carries multiple brands.

All Members utilising eftpos Secure must display the eftpos Logo and any other brandmarks as prescribed in the eftpos Brand and Style guide.

3.6. Authentication Methods and Security [Clause 3.6 is confidential]

3.7. Cardholder Verification Methods and Security [Clause 3.7 is confidential]

3.8. Form Factor BINs

a. An eftpos Form Factor must be issued with a BIN that is in the Australian Payments Network AIN-BIN Database:

   i. as an Active BIN; and

   ii. with one of the following eftpos Account Types (that represents the account selection available on the eftpos Form Factor):

      A. 1= Savings;

      B. 2 = Cheque;

      C. 4 = Savings/Cheque;

      D. 5 = Savings/Credit;

      E. 6 = Cheque/Credit; or

      F. 7 = Savings/Cheque/Credit.

b. The Company may, from time to time, prescribe requirements for eftpos Form Factors that are not eftpos Cards.

c. A Prepaid eftpos Form Factor is:

i. in the case of an eftpos Card, an eftpos Card that has the eftpos Account Type "1 = Savings" and card type "X"; and

ii. in any other case, an eftpos Form Factor that links to a prepaid account and is identified in the manner prescribed by the Company from time to time.

d. Issuers:

i. must comply with the rules and notice periods applicable to the BIN Database with respect to the addition, deletion and amendment of BINs and their associated records; and

ii. are responsible for the accuracy of the BIN Database in so far as it relates to the eftpos Cards they issue.

For the avoidance of doubt, Payment Tokens are to be issued on BINs used solely for Payment Tokens. BINs used for Payment Tokens are required to be registered in the Australian Payments Network AIN-BIN database in the same manner as all other form factor BINs. Where a Payment Token BIN is used for a Card or an eftpos Account which is to be digitised, the Payment Token BIN must carry the same attributes of the BIN of the Card or eftpos Account being digitised.

All eftpos Form Factors must be issued on BINs that allow them to be electronically identified as debit eftpos Form Factors.

3.9. BIN registration and management [Clause 3.9 is confidential]

3.10. Supported transactions

3.10.1 All eftpos Transactions

An Issuer must be capable of supporting the range of eftpos Transactions defined in the Scheme Rules for each eftpos Form Factor.

Notwithstanding Issuers rights to implement security and loss prevention controls as they see appropriate, where Issuers do apply limits to the number or value of transactions that may be performed using a specific card or form factor each day, or limits to the maximum value that may be authorised in a single transaction, Issuers must not apply different limits solely as a result of the network selected for processing of a particular transaction. For clarity, Issuers may set limits that vary by the factors including the type of transaction, whether or not cash is dispensed, and CVM methods applied, however:

a. The same daily or per transaction limits (or absence of such limits) must apply to a contactless purchase transaction performed on a Multi-Network Debit Card, regardless of which network a Merchant selects for processing of that transaction.

b. The same daily or per transaction limits (or absence of such limits) must apply to a recurring Card Not Present transaction performed on a Multi-Network Debit Card, regardless of which network a Merchant selects for processing of that transaction.

c. An Issuer must ensure parity for transaction values for online-preferred and offline capable products to maintain a consistent cardholder experience where there are multiple payments schemes on a debit card (e.g. Multi Network Debit and Multi Network Credit). Refer to the eftpos Card Application Personalisation Specification (eCAPS) for further details.

3.10.2 Chipped eftpos Cards

a. The supported transaction set must be capable of being initiated by eftpos Chip and Contactless (ACe) enabled Multi-Network Debit Cards.

b. The supported transaction set may be capable of being initiated as a contact transaction by eftpos Chip (ACe) enabled Issuer Multi-Network Credit Cards.

c. The supported transaction set must be capable of being initiated by eftpos Chip and Contactless (ACe) enabled Issuer proprietary cards.

d. The supported transaction set may be capable of being initiated by eftpos Chip and Contactless (ACe) enabled reloadable Prepaid Cards.

e. Each Issuer must ensure that each contactless eftpos Transaction initiated using a Multi-Network Debit Card is debited to the same account as a transaction from the priority application on the Multi-Network Debit Card would be debited.

f. One way the Issuer Member may do this is by implementing the optional Default Account solution made available by the Company.

3.10.3 eftpos Form Factors enabled for use in eftpos Mobile

a. Where a Mobile Wallet Provider provides a Mobile Wallet to its customers it must develop and implement the capability to:

   i. enable the Mobile Wallet Provider to elect to offer eftpos Mobile to its customers; and

   ii. support the use and lifecycle management of Payment Tokens.

b. eftpos Issuers must support Cashout using eftpos Mobile where a separate eftpos Card or virtual eftpos Card, is provisioned to a Mobile Device.

c. From the date notified by the Company, a Member may support an OEM Solution with an OEM notified by the Company as having embedded a certified eftpos applet in the Secure Element.

d. From the date notified by the Company a Member must support eftpos Mobile in all channels supported by the Member's Mobile Wallet or Member's implementation of an OEM Solution. To do this a Member must:

   i. where the Member is yet to launch a Mobile Wallet or OEM Solution, ensure that eftpos Form Factors are available as a consumer choice in and at the same time as and with parity in relation to any other payment method is made available within a Mobile Wallet or OEM Solution yet to be launched by the Member;

   ii. where the Member has already launched a Mobile Wallet or OEM Solution, undertake such activities as are required to include all eftpos Form Factors issued by the eftpos Issuer with parity in relation to any other payment method in that Mobile Wallet or OEM Solution; and

   iii. in the case of Multi-Network Cards;

      A. provide parity for eftpos Form Factors as applied to any other payment method represented or to be represented in the Mobile Wallet or OEM Solution; and

      B. comply with the eftpos Mobile Member Implementation Guide relevant to its Mobile Wallet and/or OEM Solution

3.10.4 eftpos In-App

a. Issuers using an eftpos Mobile solution must obtain certification for In-App Payments messages passing between the Issuer and eftpos Hub relating to eftpos In-App transactions initiated through eftpos Mobile. eftpos In-App Payments are considered to be eftpos Form Factor present Transactions.

b. The following Transaction types are supported for eftpos In-App Payments initiated through eftpos Mobile and must be processed in accordance with the eLS:

   i. Purchase

   ii. Refund:

      A. for transactions where Payment Token credentials are available; and

      B. for transactions where no Payment Token credentials are available, using the Card details provided by the eftpos Consumer to the Merchant at the time of processing the refund transaction. Note that any such Card-Not-Present transaction will require the Merchant, Service Provider and Acquirer to include an account type value (either CHQ/SAV). The refund will use the eftpos Digital Acceptance transaction set and data elements defined within the eLS).

c. By 1 May 2022, Issuer Members are required to support eftpos In-App Payments for device associated eftpos Payment Tokens for Multi-Network Debit cards provisioned on an OEM Solution.

3.10.5 eftpos Digital Acceptance

a. Issuer Members must obtain certification for any new message types passing between the Issuer and the eftpos Hub relating to eftpos Digital Acceptance.

b. For eftpos Digital Acceptance, support for Purchase and Refund transactions is optional from 24 April 2018, and mandatory from 22 October 2018. For clarity, this timing does not apply to eftpos Transactions at POS. To implement this, Member Issuers must be capable of receiving and responding to:

   i. Account Verify transaction (0100);

   ii. eftpos eCommerce Purchase transaction (0200);

   iii. eftpos Refund transaction (0200); and

   iv. the reversal of an eftpos Transaction processed as part of eftpos Digital Acceptance (0420).

c. From 30 April 2019, Issuer Members must also be capable of receiving and responding to the following transaction types as part of eftpos Digital Acceptance:

   i. Deposit transaction (0200); and

   ii. Withdrawal transaction (0200).

d. An Issuer must ensure that an eftpos Transaction processed through eftpos Digital Acceptance, is applied to the account that the eftpos Consumer would expect to be the source of funds for an eftpos Transaction for which they have not specifically selected eftpos CHQ or eftpos SAV.

e. From 22 October 2019, Issuer Members must complete changes necessary to support following transaction types:

   i. Payment Token request (whether received via a webservice call or message in accordance with the eftpos Hub Link Specification);

   ii. eftpos Transactions (Purchase, Refund, Deposit and Withdrawals) initiated by a Merchant or Staged Digital Wallet, using a token previously granted.

f. Prepaid Cards must not be used to perform eftpos Transactions using eftpos Digital Acceptance (other than eftpos Mobile), except where authorised by Issuer and the Company.

g. eftpos Proprietary Cards must not be used to perform eftpos Transactions using eftpos Digital Acceptance, except where authorised by the Company.

h. An Issuer must ensure that the CNP Fraud Rate does not exceed the CNP Fraud Thresholds published in the AusPayNet CNP Framework from time to time. If the Issuer's CNP Fraud Rate reaches the CNP Fraud Threshold published in the AusPayNet CNP Framework, then the Issuer must perform Strong Customer Authentication on each eftpos Digital transaction, unless the Australian Payments Network has provided the Issuer with an exemption from this requirement and the Issuer has communicated that exemption to the Company.

i. From 22 October 2019, Issuers must:

   i. consent to the allocation of Payment Tokens for PANs for which any of Recurring Payments, Instalment Payments, Deposit/Disbursement transactions or Card on File transaction functionality is available; and

   ii. approve or decline in real time any eftpos Digital transactions according to the notified availability, any requirements of Law and sufficiency funds in the relevant eftpos Consumer's account.

j. From 05 May 2020, Issuers must support and be capable of processing a Tokenisation request for Payment Tokens for a Multi-Network Debit Card. It is recommended for Issuers to enable the Token Life Cycle Management at the same time.

k. From 05 May 2021, Issuers must support and be capable of processing a Tokenisation request for Payment Tokens for an eftpos Proprietary Card. It is recommended for Issuers to enable the Token Life Cycle Management at the same time.

l. By 1 November 2021, Issuers are required to support processing of low risk Card on File Purchase and Refund transactions, as defined by eftpos CNP Standard, for Multi-Network Debit Cards, and from 1 May 2022 Issuers are required to support processing of all CNP Purchase and Refund transactions for Multi-Network Debit Cards, via the eftpos network.

m. From 1 May 2022, eftpos Issuers must support processing of low risk Card not Present Deposit and Withdrawal transactions, as defined by the eftpos CNP Standard, for Multi-Network Debit Cards, and from 1 May 2023, Issuer are required to support processing of all CNP Deposit and Withdrawal transactions for Multi-Network Debit Cards and Proprietary Cards, via the eftpos network.

3.10.6 eftpos Open Loop Transit

a. Issuer Members must obtain certification for any new message types passing between the Issuer and the eftpos Hub relating to eftpos Open Loop Transit.

b. The Company will notify Issuers of such eftpos Mobile solutions as are enabled for eftpos Open Loop Transit from time to time.

c. From 30 April 2019 Issuers must be capable of receiving and responding, and enable all of their eftpos Form Factors (excluding those determined by the Issuer as prone to Deferred Card Present decline for insufficient funds or invalid account reasons) for:

   i. Account Verify; and

ii. Purchase.

d. Account Verify and Purchase transactions used for the purposes of fare recovery are processed as Deferred Card Present transactions.

3.10.7 eQR transactions [Clause 3.10.7 is not applicable]

3.11. Statement requirements

3.11.1 Statement narrative – refund transaction

An Issuer accepts that a Refund transaction must format the Cardholder's statement narrative by using the Merchant name supplied in Field 43 of the Transaction message provided by the Acquirer.

3.11.2 Funds availability

An Issuer must apply a transaction to the eftpos Consumer's account in accordance with clauses 3.11.2.1 to 3.11.2.3 below.

A reversal of a Refund or Deposit transaction may only be sent by an eftpos Acquirer as a result of a transaction timeout or other genuine technical fault.

3.11.2.1 Withdrawal transactions

An Issuer must debit the eftpos Consumer's account in real time when a Withdrawal transaction occurs.

3.11.2.2 Refund transaction

An Issuer accepts a Refund transaction must make the funds available in real time so that the funds may be drawn upon immediately by the Cardholder.

3.11.2.3 Deposit transaction

An Issuer must credit the eftpos Consumer's account in real time when a Deposit transaction occurs.

If an Issuer receives a Disputed Transaction in respect of a Deposit transaction claiming payment to an unintended payee, then, in accordance with the ePayments Code:

a. the recipient Issuer must:

   i. co-operate in the investigation of the Deposit transaction for which a Disputed Transaction is raised;

3.11.3 Statement narrative – Short Duration Pre-Authorised transactions

To ensure compliance with the ePayments Code, Issuer should make every endeavour to ensure that both phases of the Short Duration Pre-Authorised transaction are represented as a single transaction on a cardholder's statement.

3.11.4 Issuer terms minimum requirements

Issuers must ensure that their terms with their eftpos Consumers include terms consistent with the following:

a. notification to the eftpos Consumer of the disclosures of personal information of the eftpos Consumer to effect an eftpos Transaction, or transfer of eftpos Transaction Data including collection, retention, use and disclosure by the Company of personal information of the eftpos Consumer for the purposes of processing an eftpos Transaction (including through the Company's service provider in Australia and the United States of America), involvement in and arbitration of Disputed Transactions and Chargebacks (including through the Company's service provider having databases hosted in The Netherlands and the United States of America), and for the purposes of the reporting, uses and disclosures referred to in section 9 of these Technical, Operational and Security Rules;

b. terms referencing the means of protecting minors using eftpos Form Factors and Acceptance Devices;

c. terms referencing the means of protecting eftpos Form Factors and authentication methods from unauthorised disclosure or use;

d. notification of eftpos features and functionality, including uses of eftpos Form Factors to perform all types of eftpos Transactions;

e. the timing of when the eftpos Consumer's account will be debited for an eftpos Transaction;

f. Disputed Transaction and Chargeback rights of the eftpos Consumer;

g. terms informing eftpos Consumers how Mobile Devices will be Provisioned for eftpos Mobile, including the process to be undertaken by the eftpos Consumer and the exchange of communications with the eftpos Consumer and other nominated parties that will take place, together with a statement of the nature of the information exchanged;

h. any limitations to the use of eftpos Mobile or eftpos In-App Payment, including the supported transactions for the eftpos Consumer, the availability constraints where there is diminished or no telephone reception and that there are a limited number of pre-loaded Payment Token keys that may be utilised if reception or connectivity to the eftpos Issuer host is lost, the limitations associated with the profile of the eftpos Card or eftpos Account Provisioned to the Mobile Device;

i. any rights of the eftpos Consumer, the eftpos Issuer, the OEM (as relevant) and any other party to direct a change in the Payment Token due to a lifecycle event and the process to be used by the eftpos Consumer to give effect to those rights;

j. that the Cardholder must protect their payment details and be vigilant of potential actions by fraudsters and report any suspected fraud as soon as possible to their Issuer; and

k. that the eftpos Consumer is authorised to:

   i. use or receive the benefit of the Company's Tokenisation service; and/or

   ii. use or receive the benefit of any eftpos applet embedded in an OEM Solution,

l. for the purposes of initiating and completing valid eftpos Transactions using enabled Mobile Devices, provided that the eftpos Consumer does not:

   i. grant any sublicenses to the Company's Tokenisation service software and/or eftpos applet (as the case may be;

   ii. copy, reverse engineer, decompile, disassemble, modify, adapt or make error corrections to the Company's Tokenisation service software and/or eftpos applet (as the case may be), in whole or in part; or

   iii. attempt to gain unauthorised access to any infrastructure or software used by the Company to provide the Company's Tokenisation service and/or eftpos applet (as the case may be) through any means.

A description of eftpos features and benefits is required, if another scheme's features and benefits are included. For the avoidance of doubt, descriptions of features and benefits that apply to the card no matter which scheme a transaction is routed through complies with this requirement.

These are minimum terms. Issuers may include additional terms.

3.12. Compromised cardholder data/Notifiable Incidents [Clause 3.12 is confidential]

3.13. User experience

Issuers must ensure interoperability of eftpos Form Factors, including payment system applets and applications provided to their eftpos Consumers.

Issuers providing CBP Solutions must ensure that eftpos Consumers are informed that where the Mobile Device does not have internet connectivity and all SUKs or LUCs are used or expired, that the Mobile Device cannot be used to make a purchase transaction.

Issuers participating in eftpos Secure must ensure the user experience adheres to the requirements stipulated in the relevant eftpos Secure Implementation Guides, eftpos Secure SCA User Experience Guide, and eftpos Brand and Style Guide.

3.14. Characteristics of eQR Pass Through Wallet [Clause 3.14 is not applicable]

3.15. Fraud monitoring program

The eftpos Fraud monitoring program (FMP) defines acceptable tolerances for Fraud volumes under which Issuers and Acquirers must operate. Warning and breach thresholds for the program are closely aligned to the AusPayNet CNP Fraud Framework.

Each quarter (calendar quarter), the Company will make available to each Issuer Member, a quarterly fraud reporting dashboard and portfolio quality report which outlines their performance to the program. Members who breach these programs will be required to provide the Company a Member action plan at both the warning threshold and breach threshold outlining actions being taken to bring fraud basis points below the threshold. Issuer Members are required to submit action plans within one (1) calendar month of receiving the breach notification from eftpos.

These actions plans shall be submitted via email to: fraud@auspayplus.com.au.

The program is set out below, and further requirements are referenced within the eftpos Fraud Operations Guide.

Any product	Warning threshold	Breach threshold
Approved fraud amount breach threshold (in-scope CNP transactions)	**15 bps**	**15bps**
Breach period consecutive quarters	2	3
Measurement method	• Member Fraud Reporting Dashboards and portfolio quality report.	• Member Fraud Reporting Dashboards and portfolio quality report.
Member Requirement	• Issuer Fraud Reporting via AFCX or to eftpos • Completion of Member Action Plan Template • Leveraging eftpos fraud scoring	• Issuer Fraud Reporting via AFCX or to eftpos • Completion of Member Action Plan Template • Leveraging eftpos fraud scoring
Consequence		Breach notification and fine decision as set out in the Scheme Rules – Part D Clause 16 Fines.

4. Acquirer Standards

4.1. Provision of test tools

4.1.1 eftpos Hub

The testing protocol for Direct Connections to the eftpos Hub and/or the eftpos TSP including support for eftpos Digital Acceptance and Payment Token data is set out in the Standard Hub Service Schedule.

4.1.2 Chip and Contactless

eftpos Chip and Contactless test tools are specified in the eftpos Certification Body TAV and cTAV Procedure Manual.

4.1.3 eftpos Digital Acceptance

The testing protocol and test tools for eftpos Digital Acceptance solutions are set out in the eftpos Certification Body documentation related to eftpos Digital Acceptance.

4.1.4 eftpos Mobile

As at the time these Technical, Operational and Security Rules have been published, there are no additional changes required for an Acquirer to support eftpos Mobile, therefore no test tools are required. Should additional changes be required for an Acquirer to support eftpos Mobile for Merchant Choice Routing, existing eftpos Chip and Contactless test tools will be uplifted to support this.

4.2. Use of brand marks

Except as determined by the application labelling, all Acceptance Devices must provide brand parity for the eftpos brand mark in accordance with the eftpos Brand and Style Guide as prescribed by the Company.

Any representation of the authorised eftpos Logo must be of equivalent proportions and clarity as the logo associated with any other payment choice represented in or on the relevant medium and in accordance with the eftpos Brand and Style Guide.

4.3. Secure Cryptographic Devices

Those components of a Terminal that provide services and any services involved in requesting, receiving and/or processing of the Cardholder PIN shall collectively meet the requirements of a Secure Cryptographic Device (SCD) as defined in ISO 9564-1 for on-line devices.

Additionally, SCD's must meet the requirements of AS 2805 Part 14.2 (ISO 13491-2).

4.3.1 Obligation to use compliant SCDs

In accordance with clauses 2.5.1 and 2.6.1.1, all Acquirers must use SCDs which have been approved for use by:

a. for eftpos Terminals,

   i. the PCI Security Standards Council; or

   ii. the Australian Payments Network.

b. for SCMs, the Australian Payments Network.

Acquirers are wholly responsible for ensuring that only approved eftpos Terminals and SCMs are utilised in the processing of eftpos Transactions, including those managed by their Service Providers or sponsored entities.

4.4. Terminal Key management

To the extent not inconsistent with this section, the IAC Code Set applies to Terminal key management for the purposes of the eftpos Payment System.

4.4.1 Terminal to Acquirer links

For all eftpos Terminal to Acquirer links, Acquirers must ensure that:

a. security for Transactions from Terminal to Acquirer complies with AS2805 part 6;

b. PIN security and encryption complies with AS2805 parts 3 and 5.4;

c. key management practices comply with AS2805 part 6.1;

d. message authentication must apply to all Acquirer links utilised for the transmission of eftpos Transactions;

e. the Message Authentication Code (MAC) must be calculated using, as a minimum, a DEA 3 (128-bit) key, Triple-DES and an algorithm conforming to AS2805 part 4; and

f. all PIN and MAC cryptographic functions must be performed within an SCD.

4.4.2 Key management practices [Clause 4.4.2 is confidential]

4.4.3 Rolling process for Session Keys

Session Key roll over should occur without operator intervention and in a manner compliant with AS 2805 part 6.2; AS 2805 part 6.4 or other Terminal key management protocol approved by the Company.

4.5. Cardholder data

All parties to eftpos Interchange Activities, including Acquirers; Merchants; Service Providers; intermediate network processors and third party processors, must maintain procedures and practices for preventing the unauthorised disclosure of Cardholder Data. Cardholder data includes, but is not necessarily limited to, the:

a. Primary Account Number or card number;

b. Cardholder Name;

c. Service Code;

d. Card Expiry Date; and

e. Token PAN or other Payment Token, per account or transaction as required

Acquirers and Service Providers must ensure that they, their Merchants, Service Providers, intermediate network processors and third party processors are compliant with the Payment Card Industry Data Security Standard (PCI DSS) and provide to the company on request a copy of their attestation of compliance as certified by an external Qualified Security Assessor. For Merchants participating in eftpos In-App or eftpos Digital Acceptance, Service Providers and Acquirers must monitor compliance by their Merchants and the Merchant Service Providers with the Payment Card Industry Data Security Standard (PCI DSS) on an annual basis and report the extent of compliance to the Company within 30 days of completion of each annual review.

4.6. Sensitive Authentication data

Sensitive authentication data, including but not limited to:

a. Full magnetic stripe data (or equivalent);

b. CVC2/CVV2/CID;

c. PIN or PIN Block;

d. any other form of eftpos Consumer credentials specified by the Company from time to time shall not be stored, outside of an SCD, subsequent to Authorisation.

4.7. Merchant services

4.7.1 Merchant engagement

Acquirers and Service Providers must each have in place procedures that involve the application of reasonable care and diligence so as to satisfy themselves as to the integrity, solvency and reliability of Merchants, Staged Digital Wallet Operators, third party service providers (including Processors, Payment Facilitators and Payment Aggregators), other Service Providers, which may include gateways, Token requestors and other intermediaries (including Marketplaces) in the Transaction processing or Interchange process and the owners of third party networks and devices.

Additional checks may include, but are not limited to:

a. Credit check and/or other background investigations of the business and principal owners or officers of the business, when the information in the credit check is incomplete; and

b. Inspection of the premises to verify that the prospective Merchant has the proper facilities, equipment, inventory and, where necessary, a licence or permit to conduct the business and that their nature of business matches the MCC applied for that business; and

c. in the case of eftpos Digital, in addition to the other requirements of this clause 4.7, both before commencement of provision of merchant services and periodically, but no less frequently than once per annum;

d. inspection and investigation of the online presence of the potential Authorised eftpos Digital Merchant to verify that the Merchant matches the nominated Merchant Category Code and, where necessary, holds and maintains a licence or permit to conduct the business that matches that nominated Merchant Category Code;

e. that the potential Authorised eftpos Digital Merchant meets the requirements of the eftpos CNP Standard and the requirements of these Scheme Rules;

f. that each entity satisfies the assessing entity's due diligence process as well as the requirements of the eftpos CNP Standard and the requirements of these Scheme Rules relevant to the services performed by the entity being assessed, so as not to introduce any new or increased risk to the eftpos Payment System;

g. that the Authorised eftpos Digital Merchant does not exceed the fraud thresholds prescribed in the AusPayNet CNP Framework from time to time.

4.7.2 Merchant installation

An Acquirer is responsible for providing a Merchant with the means of identifying the Merchant trading name and location on Transactions and the means of obtaining value for those Transactions.

The Merchant name and location appearing on the Record of Transaction must be the same as the Merchant name and location entered into Interchange processing (Field 43), or a meaningful truncation of it.

The agreement between the Acquirer and the Merchant and the agreement between the Merchant Service Providers and the Merchant is to refer to and require compliance with the Fraud Protection Guidelines and fraud thresholds for Merchants published by the Australian Payments Network.

4.7.3 Merchant Operating Guide

At the time of installation, the Acquirer must provide the Merchant with an Acquirer produced Merchant Operating Guide which details the various procedures relating to the processing of Transactions.

The content, format and appearance of the Merchant Operating Guide (which may embrace information relating to processing transactions for other schemes with which the Acquirer is associated) is a matter for individual Acquirers, subject to the inclusion as a minimum of the following aspects of Merchant procedures:

Requirement	Requirement detail
eftpos Digital	a. types of Transactions, solutions, infrastructure and use cases notified by the Company from time to time b. suspended or prohibited MCCs notified by the Company from time to time c. changes to fraud thresholds notified by Australian Payments Network from time to time d. minimum requirements and qualifying criteria under eftpos CNP Standard and CNP Solution Assessment Criteria.
Obligations of Merchant Service Providers	a. The obligation on the Merchant to ensure that any of its Merchant Service Providers meet the requirements of these Scheme Rules b. That the Merchant must introduce any Merchant Service Provider to have a Direct Connection to the Company to facilitate eftpos Transactions

Requirement	Requirement detail
Transactions and channels	a. The transaction types and channels being enabled for the Merchant b. any pre-requisites c. any minimum terms or conditions to the provision of services for enabled Transaction types and channels
Authorisation of each Transaction type being enabled and for each channel for the Merchant	a. when required and how obtained
Floor Limits of each Transaction type being enabled and for each channel for the Merchant	a. explanation of floor limits and fallback procedures b. not to be exceeded without authorisation
Security of information	a. prevention and notification of unauthorised attempts to i. access equipment or Consumer Data ii. procedures for detecting and reporting tampering of Acceptance Devices.
Detailed procedure for each Transaction type being enabled and for each channel enabled for the Merchant	a. completing the Transaction type, reversals and refunds from those Transaction types returns and exchanges involving eftpos sales b. Merchant settlement c. Detailed procedure for resolving Disputed Transactions and Chargebacks and reference of the eftpos Consumer to their Issuer if a Disputed Transaction is not resolved using the Merchant's refunds policy, within 180 days of the delivery date of the goods or services in the case of goods not as described d. Disputed Transaction and Chargeback rights of the eftpos Consumer e. the Merchant's right to route transactions to the payment system selected by the Merchant from available payment functionality on a Dual Network Debit Card or form factor, referencing the eftpos Logo and the wholesale pricing applicable to eftpos Transactions as published by the Company from time to time

Requirement	Requirement detail
	f. Displaying and processing any surcharging including; notifying eftpos Consumers of the amount or percentage of the surcharge per payment option, prior to payment option selection, not processing the surcharge as a Cashout and adding the surcharge to the purchase amount for purchase transactions and providing reference to requirements on limiting surcharges to "Reasonable Cost of Acceptance"
Faulty equipment	a. how to obtain service b. Fallback procedures
Minimum voucher	a. Minimum of 12 months retention period
Contact details	a. for authorisations b. Merchant service and assistance

Table 3: Merchant Operating Guide requirements

As changes occur to procedures outlined in its Merchant Operating Guide, the Acquirer must advise such changes to each of its Merchants.

4.7.4 Responsibility for Merchant compliance

The Acquirer must take such actions as are reasonably required to ensure that its Merchants, and their Merchant Service Providers, are conversant with and comply with the requirements of the procedures in these Rules applicable to Merchants.

Acquirers must:

a. monitor Merchants compliance against these Technical, Operational and Security Rules and the fraud thresholds notified in the AusPayNet CNP Framework from time to time;

b. ensure compliance with in the AusPayNet CNP Framework requirements, for CNP eftpos Transactions.

c. actively monitor such of the Acquirer's Merchants that they meet the criteria set out in 4.7.7(d) or 4.7.10.2(d) and work with the Merchants to achieve a reduction in Chargebacks, including agreeing a Chargeback reduction plan;

d. actively monitor such of the Acquirer's Merchants as notified by the Company to the Acquirer that have breached the CNP Fraud Thresholds notified in the AusPayNet CNP Framework from time to time;

e. ensure that any of the Acquirer's Merchants as notified by the Company to the Acquirer as having breached the CNP Fraud Thresholds notified in the AusPayNet CNP Framework from time to time, cease enabling eftpos Digital for that Merchant unless:

   i. Australian Payments Network has provided the Acquirer with an exemption and the Acquirer has communicated that exemption, including the basis and conditions of it to the Company; and

   ii. Notify the Company of such of the Acquirer's Merchants on the Merchant Monitoring Lists, including the steps that the Acquirer is taking with each of those Merchants to reduce Chargebacks and specifically Chargebacks under a fraud reason code. Where the relevant Merchant is a Self-Acquirer, the Self-Acquirer must notify the Company of the steps being taken by the Self-Acquirer to reduce Chargebacks.

f. ensure that any of the Acquirer's Merchants or Service Providers do not attempt to reprocess a CNP eftpos transaction processed in accordance with the eLS but was unsuccessful for any of the following reasons:

   i. the eftpos Card has expired;

   ii. the requested function is not supported;

   iii. the transaction exceeds withdrawal or purchase limits as may be applied by Issuers; or

g. ensure that any of the Acquirer's Merchants or Service Providers do not attempt to reprocess a CNP eftpos transaction, where it exceeds any withdrawal or purchase frequency limits, which the Merchant and eftpos Consumer mutually agreed to in a Payment Arrangement

Note that inclusion of an Acquirer name or ID in an eftpos Transaction message, does not constitute that Acquirer as a Merchant or Self-Acquirer for the purposes of the Scheme Rules and these Technical, Operational and Security Rules.

4.7.5 Merchant minimum qualification criteria

A Merchant receiving eftpos acceptance services must meet the following criteria, as a minimum standard, the Merchant:

a. Must have a business address in Australia or be acquired, directly or indirectly, by an Acquirer Member with a business address in Australia; and

b. must comply with any statute, regulation, semi-legislative instrument, quasi-regulation, compulsory code or voluntary code by which the Merchant is bound; and

c. must have authority, ownership, capacity and standing, to offer for use, sale, lease, licence, occupation or possession the goods or services so offered; and

d. for Deposit payments to eftpos Consumers, unless otherwise specified by the Company:

e. Merchant must comply with the Laws by which it is bound for the conduct of its business activities, including without limitation, the Anti-Money Laundering and Counter Terrorism Financing Act 2006 C'th (for example, by either becoming a reporting entity as defined within that act, or receiving specific exemption from AUSTRAC covering the solution); or

f. for an Authorised eftpos Digital Merchant, meet the requirements and qualifying criteria for eftpos Digital Acceptance as set out in the eftpos CNP Standard and sections 4.7.10 and 4.7.11 of these Technical, Operational and Security Rules; and

g. must have entered into a contract with the eftpos Acquirer or with the eftpos Acquirer's Service Provider which contains the minimum terms in 4.7.6 and is provided with an operating guide that contains the matters set out in 4.7.3 and requires the Merchant to comply with these Technical, Operational and Security Rules.

4.7.6 Acquirer minimum term requirements

Acquirers must include in their merchant contracts, terms that are consistent with the terms set out below. These are minimum terms. Acquirers may include additional terms.

Acquirers must provide:

a. notification to the Merchant of the exchanges of personal information of the Merchant to effect an eftpos Transaction, including collection, retention, use and disclosure by the Company of personal information of the Merchant for the purposes of processing an eftpos Transaction (including use of the Company's service provider in Australia and the United States of America and any other jurisdictions specified in the Company's Privacy Policy published from time to time on the Company's website), involvement in and arbitration of Disputed Transactions and Chargebacks and for the purposes of the reporting, uses and disclosures referred to in section 9 of these Technical, Operational and Security Rules;

b. a statement of the interchange rates per transaction category applicable to different payment acceptance methods or, if the Acquirer bundles all acceptance of eftpos Form Factors with any other payment acceptance method for the purposes of the fees charged to the Merchant, a statement of the interchange rate per interchange category for eftpos Transactions;

c. a statement that the Merchant has the right to elect which payments methods it accepts or accepts in preference to other payment methods;

d. that the Merchant must establish and maintain a refunds policy and disputes policy in compliance with Australian consumer laws, which at a minimum addresses consumer rights relating to:

   i. undelivered goods;

   ii. damaged or faulty goods, including a returns policy; and

   iii. goods not as described (for reasons such as lack of merchantable quality or fitness for purpose), including a returns policy;

e. that the returns policy referred to in sub-sections d) (ii) and (iii) above must provide for conclusion of any of the above claims within 180 days of the date of delivery of the goods or services (where delivered) or of the eftpos Transaction after which the eftpos Consumer is entitled to dispute the eftpos Transaction;

f. that the Merchant must display the amount or percentage of any surcharge (in accordance with rule 24 of the eftpos Scheme Rules) imposed by the Merchant per payment option, prior to payment option selection;

g. any applicable Acquirer delayed payment, withholding or security terms;

h. suspension and termination rights relating to acceptance of eftpos Transactions;

i. that the Merchant cannot:

   i. process a 0200 transaction before the goods are dispatched or allocated for dispatch or the services provided, unless otherwise notified to the eftpos Consumer in accordance to 4.7.6.d.i above a refunds policy and disputes policy for undelivered goods or services after processing a 0200 transaction;

   ii. unless otherwise authorised by the Company, process a transaction where all or part of the transaction is processed as a Cashout, where cash in the form of Australian legal tender is not provided to the eftpos Consumer. For the avoidance of doubt, any surcharge on a Transaction imposed by a Merchant must not be processed as a Cashout; and

   iii. after end of October 2017, impose a minimum value for the acceptance of eftpos Transactions.

j. Where required by Law, and in accordance with Law, any Merchant exercising their right to choose a payment application present and available on a Multi-Network Debit Card must inform the Cardholder that if they wish to select a specific network then they should insert their card and select from the available options.

k. Any reference to the eftpos Payment System must use the eftpos Logo.

l. that the Merchants are aware that eftpos Form Factors can be allocated to minors.

4.7.7 Suspension of Merchants

An Acquirer must suspend a Merchant (whether or not connect directly to the Acquirer) pending resolution in the following circumstances:

a. on death or insolvency of the Merchant;

b. if the Merchant commits or is suspected of committing a breach of laws, including without limitation fraud, cartel conduct, money laundering, corrupt activities, terrorist activities;

c. if the Merchant provides goods or services of a nature that are or would result in a breach of laws;

d. if the Company has notified the Acquirer that the Merchant or category of Merchant to which a Merchant belongs introduces an unacceptable risk or increase in risk, or diminishes the reputation of the eftpos Payment System, which may include (without limitation)

   i. category of Merchant;

   ii. disputed Transaction and Chargeback history for a specific Merchant or Merchant category;

   iii. disputed Transaction and Chargeback trends, Merchant category mix, adverse financial impacts on an Acquirer of any of the above; or

   iv. adverse impacts on the reputation, security, viability or regulatory compliance standing of the Company or the eftpos Payment System

e. if the Merchant exceeds the fraud mitigation thresholds and measures set by the Company from time to time;

f. In accordance with AusPayNet CNP Fraud Framework and relevant documentation.

These are minimum standards. Acquirers may set additional criteria for Merchant suspension or termination at their discretion. An Acquirer must terminate a Merchant if any of the above is not capable of resolution.

4.7.8 Returned merchandise and adjustments

The Acquirer must require that if:

a. any merchandise purchased with an eftpos Form Factor is accepted for return or any services are terminated or cancelled, or any price adjustment made, the Merchant must affect an eftpos Form Factor based refund transaction, rather than a cash-based refund. The Payment Facilitator program participants may initiate and process either a Manual Entry refund with the Cardholder present, or. a CNP Refund Transaction, based on their specific business model and appropriately implemented risk control measures; and

b. any merchandise purchased using eftpos Digital Acceptance is accepted for return or any services are terminated or cancelled, or any price adjustment made, the Merchant must affect a refund transaction using eftpos Digital Acceptance, rather than a cash or form factor based refund for returned goods or Transactions processed after the date on which the service is terminated or cancelled.

4.7.9 Multiple sales transactions and partial considerations

The Merchant must include all items, goods and services purchased in a single transaction for the total amount of such purchases, except in the case of purchases in separate departments within a retail outlet or in the case of a partial payment or delayed delivery situation when:

a. the balance of the amount due is paid by the Cardholder at the time of the sale by another means; or

b. during down time, the Cardholder executes two separate sales vouchers in a delayed delivery sale. If the amount of both sales vouchers exceeds the Merchant's floor limit the Merchant must seek Authorisation for the value of each sales voucher from the Acquirer's processing centre. If Authorisation is obtained, the Transaction must be assigned separate Authorisation numbers for each sales voucher.

4.7.10 Criteria for eftpos Digital Acceptance

eftpos Digital Acceptance allows an eftpos Transaction to be processed in a Card-Not-Present environment, utilising some or all of the following according to the CNP Standard:

a. a Digital Acceptance Device;

b. a Payment Token, or Acquiring Token;

c. Domain Controls;

d. Cardholder Authentication;

e. Transaction Authentication.

Each implementation of eftpos Digital Acceptance by an Acquirer or Self-Acquirer, must be submitted by the Acquirer for review by the Company against the minimum criteria set out in the eftpos CNP Standard and can only be implemented as an Approved Digital Acceptance Solution under eftpos Trade Marks if approved by the Company.

The Company will publish to Members:

a. the solution proposed in an application for review of an eftpos Digital Acceptance solution;

b. the eftpos CNP Standard; and

c. a listing of Approved Digital Acceptance solutions.

An Acquirer or Self-Acquirer offering an Approved Digital Acceptance Solution (whether or not connected directly with the Merchant) must provide reporting to the Company in accordance with clause 9.1.5 of these Technical, Operational and Security Rules.

4.7.10.1 Merchant minimum qualification criteria for eftpos Digital Acceptance

a. An Acquirer must ensure that an Authorised eftpos Digital Merchant receiving eftpos Digital Acceptance services meets the following criteria, as a minimum standard. In addition to the criteria in clause 4.7.5, the Authorised eftpos Digital Merchant:

  i. no longer used:

    A. no longer used

    B. no longer used

  ii. must demonstrate, to the Acquirer on enquiry, terms and conditions and policies that clearly articulate the customer enrolment, customer identification and verification checks on enrolment and throughout any Payment Arrangement period, credit limit setting, risk scoring and risk management, the Merchant's refunds policy, customer service and support and high levels of integrity in the application of their refund policy and any past disputed transaction resolution;

  iii. falls within one of the MCCs and Transaction types defined within the eftpos CNP Standard as published by the Company from time to time;

  iv. demonstrate existing robust procedures relating to initial and ongoing Cardholder Authentication, and in the case of Merchants providing Deposit transactions know your customer (KYC) identification and verification procedures, which meet the requirements of the eftpos CNP Standard, at the time of:

    A. setting up an eftpos Consumer account;

    B. enrolling an eftpos Consumer into a contracted-service in respect of which eftpos Transactions will be initiated; or

    C. expanding service offerings to an existing eftpos Consumer;

    D. if the Merchant's Chargebacks under a fraud reason code exceed the levels set out in the AusPayNet CNP Framework;

    E. if the card has not been used within the last 180 days

  v. must demonstrate compliance and must maintain ongoing compliance with PCI DSS;

  vi. for at least 12 months, unless otherwise notified by the Company:

    A. must have been initiating card payments, including the type of payments for which the Merchant is enabled;

    B. must have maintained acceptable fraud levels within AusPayNet CNP Framework on a per calendar quarter basis and must not have appeared on any payment network's non-compliance reporting – notification and/or enforcement; and

C. must have maintained acceptable Chargeback levels within the requirements of 4.7.10.2 of these Technical, Operational and Security Rules.

vii. Note: For the purposes of this calculation, chargebacks include both fraud and non-fraud related customer disputes;

viii. must display the price for all eftpos Transactions to the eftpos consumer at the time of Purchase and processing and, if necessary, Refund in AUD;

ix. must pay the full AUD amount for any refunded eftpos Transactions or any eftpos Transactions to which a Chargeback applies; and

x. must have entered into a contract with the eftpos Acquirer which contains the minimum terms in 4.7.6 and 4.7.10 and be provided with an operating guide that contains the matters set out in 4.7.3.

4.7.10.2 When Acquirers cannot offer eftpos Digital Acceptance

eftpos Acquirers cannot provide eftpos Digital Acceptance services to the following:

a. Merchants (whether or not connected directly to the Acquirer) that do not meet the criteria set out in 4.7.10.1;

b. Extreme Risk Merchant categories specified in the eftpos CNP Standard as published by the Company from time to time;

c. Merchants with more than:

   i. 0.5% estimated Disputed Transactions deemed as fraud made in respect of any payment method where the Merchant has not previously used eftpos Digital Acceptance; or

   ii. 0.5% Disputed Transactions deemed as fraud made in respect of Purchase transactions where the Merchant offers eftpos Digital Acceptance; or

   iii. 0.5% Disputed Transactions deemed as fraud made in respect of Withdrawal transactions where the Merchant offers eftpos Digital Acceptance,

   iv. Initiated with them in the last 12 months unless additional controls are implemented by the Acquirer or Self-Acquirer to bring Disputed Transaction levels back below the thresholds specified above within 6 months.

d. Merchants, where during any two consecutive Quarters in the preceding 12 months, in respect of any payment method, has charged back transactions representing 2% or more of total transaction volume across all channels in a single month;

e. Merchants, where for four consecutive Quarters in the preceding 12 months have exceeded the CNP Fraud Thresholds published in the AusPayNet CNP Framework from time to time unless:

i. AusPayNet has provided the Acquirer with an exemption and the Acquirer has communicated that exemption, including the basis and conditions of it to the Company.

f. Merchants that are known or suspected by the Acquirer of committing actual or suspected breach of laws, including without limitation fraud, cartel conduct, money laundering, corrupt activities, terrorist activities;

g. Merchants that are suspended by the Acquirer for actual or suspected breach of laws, including without limitation fraud, cartel conduct, money laundering, corrupt activities, terrorist activities;

h. Merchants that repeatedly breach and fail to implement a rectification plan for non-compliance with the eftpos Technical, Operational and Security Rules;

i. Merchants that introduce an unacceptable risk or an unacceptable increase in risk for the eftpos Payment System, including without limitation if the Merchant (that is also a Self-Acquirer) falls out of compliance with PCI DSS;

j. Merchants that bring the eftpos Payment System into disrepute;

k. Merchants that cause the Company or an Issuer to be in breach of a law; or

l. Merchants as communicated at the discretion of the Company where the Merchant's behaviour (e.g. selling prohibited goods, terminated merchant with other Acquirers) is outside of the risk appetite of the Company.

4.7.10.3 Authorised eftpos Digital Merchant minimum terms

Acquirers must include terms consistent with the following minimum terms in their contracts with Authorised eftpos Digital Merchants whether acquired directly or through any Processor or Service Provider used for eftpos Digital Acceptance by an Authorised eftpos Digital Merchant:

a. any applicable Acquirer delayed payment, withholding terms or security terms;

b. suspension and termination rights – relating to eftpos Digital Acceptance;

c. the Authorised eftpos Digital Merchant cannot process a Purchase transaction before an inventory check is completed and the goods are allocated to the order or the services provided;

d. the Authorised eftpos Digital Merchant must publish on its website the transaction the availability of transaction receipts and delivery receipt requirements related to the goods or services (e.g. when identification is required on delivery); and

e. where the transaction is for the purchase of goods requiring physical delivery, the Authorised eftpos Digital Merchant must obtain from the eftpos Consumer details or confirmation of the delivery address at the time of each eftpos Transaction;

f. Merchant must be able to provide a record of the authority granted by the Cardholder to allow future Merchant Initiated Transactions (e.g. Fixed Frequency, Pay As You Go, Instalment, Deferred Payments or Post Payment Adjustments) by that Merchant;

g. Merchant must be able to provide a record of the authority granted by the Cardholder to the Merchant to perform transactions in a Payment Arrangement; and

h. for CNP eftpos Transactions, requirements that the Merchant published terms and conditions must include where applicable:

   i. term and termination rights;

   ii. payment terms, including transaction type, any limits on the individual and cumulative amount, number and frequency of payments, minimum and maximum contract period, including expiry date;

   iii. delivery and shipping terms, for payments associated with purchase of goods

   iv. reversal, full and partial refunds and corrections procedure;

   v. eftpos Consumer rights if expected Deposit payments are not received;

   vi. rights to amend, cancel or dispute payments;

   vii. Payment date for eftpos Consumer;

   viii. procedure for the eftpos Consumer to notify change of Card or account details; and

   ix. Customer service details.

4.7.10.4 Authorised eftpos Digital Merchant requirements

Acquirers must ensure that their Authorised eftpos Digital Merchants adhere to the eftpos Digital Acceptance requirements set out in this clause 4.7.10.4, whether directly or through any Processor or Service Provider used for eftpos Digital Acceptance by an Authorised eftpos Digital Merchant.

Acquirers must ensure that their Authorised eftpos Digital Merchants:

a. perform Strong Customer Authentication for eftpos Digital transactions in a manner which meets the requirements of the AusPayNet CNP Framework, unless otherwise communicated by the Company;

b. operate through an Approved Digital Acceptance Solution that meets the requirements of these Technical, Operational and Security Rules;

c. do not require account level selection on the checkout screen;

d. do not process a reversal of a Refund or Deposit Transactions, other than as a result of a transaction timeout or other genuine technical fault or as a result of a Disputed Transaction;

e. must request the CVV on the Card to be entered for guest checkout or non-Card On File eftpos Transactions;

f. must have in place a policy for Cardholder Authentication from time to time that is consistent with these Technical, Operational and Security Rules and approved under the eftpos CNP Standard, to minimise the risk of fraud;

g. only initiate an eftpos Transaction with a valid eftpos Form Factor and where the Merchant has satisfied the Acquirer that they meet the requirements of (f) above or Transaction Authentication by Issuer has been performed, in each case by a method approved by the Company;

h. disable the eftpos Consumers log in to the account with the Authorised eftpos Digital Merchant at the earlier of:

   i. a request to do so by the eftpos Consumer;

   ii. where the eftpos Consumer commits or is suspected of committing a breach of laws, including without limitation fraud, money laundering, corrupt activities, terrorist activities;

   iii. when the Registered eftpos Consumer logs out of the Registered eftpos Consumer's account with the Authorised eftpos Digital Merchant.

i. only obtain payment Card details for the following purposes:

   i. to request an Acquiring Token from an Acquirer, Self-Acquirer or Processor that that is an Approved Digital Acceptance Solution;

   ii. to perform a one-off payment transaction in conjunction with a Transaction Authentication service approved by the Company; and

   iii. to request an eftpos Payment Token from an eftpos authorised Token Requestor, that is an Approved Digital Acceptance Solution.

j. do not store in a record a PAN and discard all payment card details at the earlier of:

   i. when the Token has been provided to the Merchant; or

   ii. when the Transaction has been completed;

k. who utilise a Service Provider which is not in itself an Approved Digital Acceptance Solution, ensure that Service Provider:

   i. has an agreement with an Acquirer ; and

   ii. meets the minimum criteria set out in the eftpos CNP Standard;

l. have fraud and risk management capability, or use the fraud and risk management capability provided by the Acquirer, Self-Acquirer or Processor in accordance with the eftpos CNP Standard;

m. unless otherwise approved by the Company, a funding of another payment facility can only be done using a Withdrawal transaction, not Single Payment or other payment under a Payment Arrangement;

n. have a proactive and reactive method for:

   i. in respect of all eftpos Digital payment types, customer identification and verification;

   ii. in respect of Payment Arrangements, fraud identification, fraud scoring, rules-based fraud detection, delay on shipping for suspicious purchases and Merchant's own Strong Customer Authentication and due diligence on any service user;

   iii. in respect of Instalment Payments, credit and bad debt management, such as the maximum number of parallel Instalment Payment plans that may be in place at one time per account with that Merchant;

o. for Merchant Initiated Transactions:

   i. except for Approved eftpos Digital Solutions, perform positive Cardholder Authentication using an eftpos approved Strong Customer Authentication method before retaining or using eftpos Consumer's Card or Token details for future Merchant Initiated transactions;

   ii. the first payment request in an existing series of the payments or new series of payments must be presented and completed using an eftpos approved Cardholder Authentication method;

   iii. Cardholder Authentication is not required to be completed on transactions routed via the eftpos Hub where a previous transaction was routed via another payment network and Cardholder Authentication was successfully and recently completed in accordance with the AusPayNet CNP Framework. Examples of acceptable Cardholder Authentication are:

      A. for transactions re-routed via the eftpos Hub, where previous transactions in the series were routed via another payment network and Cardholder Authentication was successfully completed within the last 3 months in accordance with AusPayNet CNP Framework; or

      B. for new transactions, Issuer ID&V or Transaction Authentication by Issuer, evidenced to the Acquirer or Merchant by an authorisation approval response and completion of a tokenised financial transaction in real time;

   iv. obtain acknowledgement from the eftpos Consumer that they authorise the Merchant to retain the eftpos Consumer's Card or Token details and to use them for initiating transactions in future;

   v. at the time that the eftpos Consumer is asked to provide authority, inform the eftpos Consumer of the extent of the authority which the eftpos Consumer is granting to the Merchant to retain the eftpos Consumer's Card details and initiate future Merchant Initiated Transactions, and Purchases using Card on File, including

      A. the amount of each Transaction (whether fixed amount or how the amount to be charged is calculated);

      B. the frequency of Transactions and schedule of Transactions (where known);

C. The final date that Transactions can be charged;

D. the methods by which the eftpos Consumer may withdraw consent for further Transactions to be performed using their Card or the eftpos Consumer or the Merchant may terminate the agreement for provision of goods or services

E. all associated fees for service (including but not limited merchant dishonour fee, cancellation fee etc.) that can be included in the Transaction amount;

vi. not to process a Post-Payment Adjustment Transactions after 30 days of the original transaction.

vii. not initiate any eftpos Transactions other than for the purposes, and within the time period that was agreed with or notified by the eftpos Consumer;

viii. For Merchants initiating a Transaction as permitted by these Technical, Operational and Security Rules, have operational processes (e.g. contacting eftpos Consumer to seek alternate payment methods, and/or cancelling dispatch of goods) to cater for any Transactions that are declined by the Issuer; and

ix. ensure a Merchant performs Cardholder Authentication via eftpos Secure after the date notified by the Company and shall not continue to perform eftpos Digital transactions from those Merchants if:

A. the Chargeback ratios exceed the thresholds set out in these Technical, Operational and Security Rules; or

B. the Merchant exceeds the fraud threshold(s) specified in the AusPayNet Card Not Present Fraud Mitigation Framework for three consecutive quarters.

x. must ensure the use of the correct BAI value that represents the real intention of the Deposit/Withdrawal transaction is present in the authorisation request.

xi. ensure that any of the Acquirer's Merchants or Service Providers do not attempt to reprocess a CNP eftpos Transaction processed in accordance with the eLS but was unsuccessful for any of the following reasons:

A. the eftpos Card has expired;

B. the requested function is not supported

C. the transaction exceeds withdrawal or purchase limits as may be applied by Issuers;

D. A permanent decline

xii. ensure that any of the Acquirer's Merchants or Service Providers do not attempt to reprocess a CNP eftpos transaction, where it exceeds any withdrawal or purchase frequency limits, which the Merchant and eftpos Consumer mutually agreed to in a Payment Arrangement.

xiii. Other than in accordance with xi above, a Merchant may resubmit that transaction, no more than once per Calendar Day, up to a maximum of 4 retries over a period of 16 Calendar Days from the original declined transaction date.

4.7.10.5 Authorised Staged Digital Wallet Operator minimum terms

Acquirers must include terms consistent with the following minimum terms in their contracts with Authorised Staged Digital Wallet Operators (whether directly or through any Processor or Service Provider used for eftpos Digital Acceptance):

a. notification to the Staged Digital Wallet Operator of the exchanges of any personal information of the Staged Digital Wallet Operator (and cause the Staged Digital Wallet Operator to notify their End Merchants) required to process an eftpos Transaction, Disputed Transactions and Chargeback, including collection, retention, use and disclosure by the Company of personal information consistent with the Company's Privacy Policy published from time to time on the Company's website), involvement in and arbitration of Disputed Transactions and Chargebacks and for the purposes of the reporting, uses and disclosures referred to in section 9 of these Technical, Operational and Security Rules;

b. a statement of the interchange rates per transaction category applicable to different payment acceptance methods or, if the Acquirer bundles all acceptance of eftpos Form Factors with any other payment acceptance method for the purposes of the fees charged to the Staged Digital Wallet Operator, a statement of the interchange rate per interchange category for eftpos Transactions;

c. a statement that the Staged Digital Wallet Operator has the right to elect which payments methods it accepts or accepts in preference to other payment methods;

d. that the Staged Digital Wallet Operator must establish and maintain a refunds policy and disputes policy in compliance with Australian consumer laws, which shall apply to all purchases at the End Merchants paid for by an eftpos Form Factor loaded into the Staged Digital Wallet and at a minimum addresses consumer rights relating to:

   i. undelivered goods;

   ii. damaged or faulty goods, including a returns policy; and

   iii. goods not as described (for reasons such as lack of merchantable quality or fitness for purpose), including a returns policy;

e. that the returns policy referred to in sub-sections d) (ii) and (iii) above must provide for conclusion of any of the above claims within 180 days of the date of delivery of the goods or services (where delivered) or of the eftpos Transaction, after which the eftpos Consumer is entitled to dispute the eftpos Transaction;

f. that the Staged Digital Wallet must display the amount or percentage of any surcharge (in accordance with rule 24 of the eftpos Scheme Rules) imposed by the Staged Digital Wallet Operator per payment option, prior to payment option selection;

g. any applicable Acquirer delayed payment, withholding or security terms;

h. suspension and termination rights relating to acceptance of eftpos Transactions;

i. that the Staged Digital Wallet Operator cannot:

  i. process a 0200 transaction before being notified by the End Merchant that the goods are dispatched or allocated for dispatch or the services provided; and

  ii. impose a minimum value for the acceptance of eftpos Transactions.

j. No longer used.

k. No longer used.

l. No longer used.

m. Staged Digital Wallet Operators need to be aware that eftpos Form Factors can be allocated to minors and must have relevant restrictions and terms in place for age-prohibited goods or services to eftpos Cardholders who may be minors.

4.7.10.6 Authorised Staged Digital Wallet requirements

Acquirers must ensure that their Authorised Staged Digital Wallets Operator adhere to the eftpos Digital Acceptance requirements set out in this clause 4.7.10.6, whether directly or through any Processor or Service Provider used for eftpos Digital Acceptance. Acquirers must ensure their Authorised Staged Digital Wallet Operators:

a. No longer used:

b. must meet the minimum criteria set out in the eftpos CNP Standard;

c. must provide the following facilities:

  i. electronic facility that allows eftpos Consumers to raise Disputed Transactions with the Staged Digital Wallet Operator, and for such disputes to be resolved between cardholder and the Staged Digital Wallet.

  ii. electronic facility that allows cardholders to determine which specific goods and services were paid for via an individual transaction, and the funding source(s) (including payment scheme) which was used to make such payment

d. Any eftpos CNP Transaction originating in Staged Digital Wallet, for a Purchase or Refund on behalf of an End Merchant, shall be formatted

i. With the 'Merchant Name\Location' field identifying both the wallet, and the End Merchant. For clarity, it is not required to identify a physical location for the End Merchant in this field; and

ii. With a Merchant Category Code set to the value defined within AS2805.16 which most accurately reflects the specific End Merchant providing goods or services to the cardholder.

e. must be able to support receiving Disputed Transactions directly from an Issuer, using the eftpos Disputes and Chargeback Tool or any other tool nominated by the Company from time to time, without needing to be passed to the Acquirer first. (Acquirer shall remain directly liable for all Chargebacks to Staged Digital Wallet eftpos Transactions that they process, irrespective of whether or not the Acquirer is able to recover such Chargebacks from the Staged Digital Wallet Operator)

f. must meet the qualifying conditions for End Merchants located outside Australia:

i. ensure (via the End Merchant's Terms & Conditions) that the eftpos Consumers receive the same consumer protection as would apply had the End Merchant been located within Australia and subject to Australian law;

ii. the eftpos Consumer is advised about the Transaction amount in the Australian dollars before the eftpos Transaction is initiated and any Refund is to be in the full Australian dollar Purchase amount without deduction;

iii. must process the eftpos Transaction with a correct AS 2632 Country Code of the country where the End Merchant is located;

iv. and must not process any transactions originating from the entities or countries under current sanction published by the Australian Department of Foreign Affairs and Trade as notified by the Company from time to time. The Acquirers authorise the Company to reject all prohibited transactions at the eftpos Hub.

4.7.10.7 Suspension of Staged Digital Wallet Operators

An Acquirer must suspend a Staged Digital Wallet Operator pending resolution in the following circumstances:

a. on death or insolvency of the Staged Digital Wallet Operator;

b. if the Staged Digital Wallet Operator commits or is suspected of committing a breach of laws, including without limitation fraud, cartel conduct, money laundering, corrupt activities, terrorist activities;

c. if the Staged Digital Wallet Operator allows payments to be made to an End Merchant which provides goods or services of a nature that are or would result in a breach of laws;

d. In accordance with AusPayNet CNP Fraud Framework and relevant documentation; or

e. if the Staged Digital Wallet Operator exceeds the fraud mitigation thresholds and measures set by the Company from time to time.

These are minimum standards. Acquirers may set additional criteria for Staged Digital Wallet Operator suspension or termination at their discretion. An Acquirer must terminate a Staged Digital Wallet Operator if any of the above is not capable of resolution.

4.7.10.8 Minimum qualification criteria for Installment Payment Solution Providers

a. An Acquirer may facilitate the provision of eftpos Digital to Merchants through Merchant Service Providers that provide Instalment Payment solutions either directly through a proprietary Instalment Payment solution or indirectly via a third-party Instalment Payment solution provider to Merchants. In that case, both the Merchant Service Provider that provides Instalment Payment solutions and the End Merchant are Merchants for the purposes of these Technical, Operational and Security Rules. As such, the provisions of 4.7.10.2, 4.7.10.3, 4.7.10.4 also apply to the Acquirer in respect of the Merchant Service Provider that provides Instalment Payment solutions as if it is the Merchant.

b. An Acquirer must satisfy itself that a Merchant Service Provider that is an Instalment Payment solution provider:

i. meets and demonstrate that they meet the requirements of any laws applicable to the nature of the business conducted by it;

ii. No longer used;

iii. demonstrates, to the Acquirer on enquiry, terms, conditions and policies that clearly articulate the customer enrolment, customer identification and verification checks on enrolment and throughout instalment period, credit limit setting, risk scoring and risk management, customer service and refunds policy, identification and qualification checks for participating Merchants, clear Merchant contract, documented Merchant enrolment and education program, cancellation policy, pre and post instalment communications and high levels of integrity in the application of their refund policy and customer service;

iv. maintains and have maintained for the 3 or more months of the immediately preceding 12 months before their acceptance for eftpos Digital, their aggregate performance within the fraud threshold(s) specified in the AusPayNet Card Not Present Fraud Mitigation Framework and has not appeared in any payment network non-compliance reporting – notification and enforcement;

v. demonstrates existing robust procedures relating to initial and ongoing Cardholder Authentication procedures, which meet the requirements of the CNP Standard, at the time of:

A. setting up an eftpos Consumer account;

B. enrolling an eftpos Consumer into a contracted-service in respect of which eftpos Transactions will be initiated; or

C. expanding service offerings to an existing eftpos Consumer;

D. if the Merchant's Chargebacks under a fraud reason code exceed the levels set out in these Technical, Operational and Security Rules;

vi. demonstrates compliance and must maintain ongoing compliance with PCI DSS;

vii. displays the price for all eftpos Transactions to the eftpos consumer at the time of Purchase and processing and, if necessary, Refund in AUD;

viii. pays the full AUD amount for any refunded eftpos Transactions or any eftpos Transactions to which a Chargeback applies;

ix. only provides Instalment Payment services for eftpos Digital to Merchants that meet the MCCs and within the limits specified by the Company from time to time;

x. has entered into a contract with the eftpos Acquirer. For clarity, where the Merchant Service Provider indirectly provides an Instalment Payment solution via a third-party, a contract between the eftpos Acquirer and third-party Instalment Payment solution provider is not required; and

xi. shall format any eftpos CNP Transaction processed by the Instalment Payments service provider for a Purchase or Refund on behalf of an End Merchant:

A. With the 'Merchant Name\Location' field identifying both the Instalment Payment solution provider, and the End Merchant. For clarity, it is not required to identify a physical location for the End Merchant in this field; and

B. With a Merchant Category Code set to the value defined within AS2805.16 which most accurately reflects the specific End Merchant providing goods or services to the cardholder.

4.7.11 Criteria for eftpos In-App Payments

4.7.11.1 Merchant minimum qualification criteria for eftpos In-App Payments

An Acquirer must ensure that an Authorised eftpos Digital Merchant processing eftpos In-App Payments as part of eftpos Mobile meets the following criteria, as a minimum standard. In addition to the criteria in clause 4.7.5 the Authorised eftpos Digital Merchant:

a. must operate through a, Digital Acceptance Device which meets the requirements of these Technical, Operational and Security Rules;

b. must display the price for all eftpos Transactions to the eftpos Consumer at the time of purchase and processing and, if necessary, refund in AUD;

c. must pay the full AUD amount for any refunded eftpos Transactions or any eftpos Transactions to which a Chargeback applies;

d. has entered into a contract with the Acquirer which contains the minimum terms in 4.7.6 and 4.7.10 and is provided with an operating guide that contains the matters set out in 4.7.3;

e. has all required licences, consents and authorities to accept eftpos In-App Payments;

f. displays the payment acceptance icon for any OEM Solutions accepted as a payment option in the Authorised eftpos Digital Merchant application for which the eftpos Form Factor is available as a payment option;

g. only offers the ability to accept eftpos In-App Payments where:

   i. the eftpos Transaction is initiated with a valid Payment Token allocated to the eftpos Form Factor by the eftpos TSP, eligible for use in an OEM Solution that supports eftpos In-App Payments;

   ii. the eftpos Consumer has confirmed that they are authorised to use the eftpos Form Factor; and

   iii. where the Transaction is a type approved by the Acquirer.

4.7.11.2 When Acquirers cannot offer eftpos In-App Payments

eftpos Acquirers cannot provide eftpos In-App Payments services to the following:

a. Merchants that do not meet the criteria set out in 4.7.11.1;

b. No longer used.;

c. Merchants exceeding the Chargeback criteria in clause 4.7.7 d);

d. Merchants that are known or suspected by the Acquirer of committing actual or suspected breach of laws, including without limitation fraud, cartel conduct, money laundering, corrupt activities, terrorist activities;

e. Merchants that are suspended by the Acquirer for actual or suspected breach of laws, including without limitation fraud, cartel conduct, money laundering, corrupt activities, terrorist activities;

f. Merchants that repeatedly breach the eftpos Technical, Operational and Security Rules;

g. Merchants that introduce a risk or an unacceptable increase in risk for the eftpos Payment System;

h. Merchants that bring the reputation of the eftpos Payment System into disrepute; or

i. Merchants that cause eftpos or an Issuer to be in breach of a law.

4.7.11.3 Authorised eftpos Digital Merchant minimum terms – eftpos In-App Payments

eftpos Acquirers must include terms consistent with the following minimum terms in their contracts with Authorised eftpos Digital Merchants (and any Service Provider utilised by the Authorised eftpos Digital Merchant) relating to eftpos In-App Payments:

a. any applicable Acquirer delayed payment, withholding terms or security terms;

b. suspension and termination rights – relating to eftpos In-App Payments;

c. the Authorised eftpos Digital Merchant cannot process a 0200 transaction before an inventory check is completed and the goods are allocated to the order or the services provided;

d. the Authorised eftpos Digital Merchant must make available through the OEM Solution or Authorised eftpos Digital Merchant's website, mobile application or via email to the Registered eftpos Consumer the transaction receipt and delivery receipt requirements related to the goods or services (e.g. when identification is required on delivery);

e. the Authorised eftpos Digital Merchant must only deliver goods to an eftpos Consumer using eftpos In-App Payments as part of an OEM Solution where the Authorised eftpos Digital Merchant obtains a statement or confirmation of the delivery address as part of the transaction.

f. The Merchant must be able to provide a record of the authority granted by the Cardholder to allow future Merchant Initiated Transactions (e.g. Fixed Frequency, Pay As You Go, Instalment, Deferred Payments or Post-Payment Adjustments) by that Merchant;

g. The Merchant must be able to provide a record of the authority granted by the Cardholder to the Merchant to perform transactions in a Payment Arrangement; and

h. requirements that the Merchant published terms and conditions must include where applicable:

   i. term and termination rights;

   ii. payment terms, including transaction type, any limits on the individual and cumulative amount, number and frequency of payments, minimum and maximum contract period, including expiry date;

   iii. delivery and shipping terms, for payments associated with purchase of goods

   iv. reversal, full and partial refunds and corrections procedure;

   v. rights to amend, cancel or dispute payments;

   vi. Payment date for eftpos Consumer;

   vii. procedure for the Registered eftpos Consumer to notify change of payment or account details; and

viii. Customer service details.

4.7.11.4 Authorised eftpos Digital Merchant requirements – eftpos In-App Payments

Acquirers must ensure that their Authorised eftpos Digital Merchants (and any Service Provider utilised by the Authorised eftpos Digital Merchant) adhere to the applicable OEM Solution and eftpos In-App Payments Member Implementation Guide for eftpos In-App Payments.

Acquirers must ensure that an Authorised eftpos Digital Merchant offering eftpos In-App Payments for an OEM Solution:

a. has all required licences, consents and authorities to accept eftpos In-App Payments;

b. have implemented a solution for Tokenisation in accordance with Section 5 of these Technical, Operational and Security Rules;

c. are themselves or through their Service Provider (as relevant) either fully compliant with PCI DSS and are capable of producing satisfactory evidence of that compliance on request or do not collect and store in a record any PAN or Payment Token;

d. utilise a Service Provider which meets the requirements of these Technical, Operational and Security Rules;

e. have and utilise for eftpos Transactions, fraud and risk management capability in accordance with the eftpos In-App Payments Member Implementation Guide issued by the Company from time to time;

f. enables the selection by the eftpos Consumer of the eftpos Form Factor as the payment method for an In-App transaction, whether or not the eftpos Form Factor is the default form factor identified for the purposes of the relevant Mobile Device enables the selection by the eftpos Consumer of the eftpos Form Factor as the payment method or an in-app transaction, whether or not the eftpos Form Factor is the default form factor identified for the purposes of the relevant Mobile Device; and

g. complies with the eLS for messages initiated using eftpos In-App, specifically that both cryptogram for the eftpos Consumer's Mobile Device and the Payment Token allocated by the eftpos TSP form part of the eftpos Transaction, and

h. for Merchant Initiated Transactions:

   i. the first payment request in an existing series of the payments or new series of payments must be presented and completed using with positive Cardholder Authentication via Consumer Device Cardholder Verification Method (CDCVM);

ii. Cardholder Authentication is not required to be completed on transactions routed via the eftpos Hub where a previous transaction was routed via another payment network and Cardholder Authentication was successfully and recently completed;

iii. obtain acknowledgement from the eftpos Consumer that they authorise the Merchant to retain the eftpos Consumer's Payment Token details and to use them for initiating transactions in future;

iv. at the time that the eftpos Consumer is asked to provide authority, inform the eftpos Consumer of the extent of the authority which the eftpos Consumer is granting to the Merchant to retain the eftpos Consumer's Form Factor details and initiate future Merchant Initiated Transactions, and Purchases using Card on File, including

   A. the amount of each Transaction (whether fixed amount or how the amount to be charged is calculated);

   B. the frequency of Transactions and schedule of Transactions (where known);

   C. The final date that Transactions can be charged;

   D. the methods by which the eftpos Consumer may withdraw consent for further Transactions to be performed using their eftpos Form Factor, or the eftpos Consumer or the Merchant may terminate the agreement for provision of goods or services

   E. all associated fees for service (including but not limited merchant dishonour fee, cancellation fee etc.) that can be included in the Transaction amount;

v. not to process a Post-Payment Adjustment Transactions after 30 days of the original transaction.

vi. not initiate any eftpos Transactions other than for the purposes, and within the time period that was agreed with or notified by the eftpos Consumer;

vii. have operational processes (e.g. contacting eftpos Consumer to seek alternate payment methods, and/or cancelling dispatch of goods) to cater for any Transactions that are declined by the Issuer;

viii. ensure that any of the Acquirer's Merchants or Service Providers do not attempt to reprocess an eftpos In-App Payment processed in accordance with the eLS but was unsuccessful for any of the following reasons:

   A. the eftpos Form Factor has expired;

   B. the requested function is not supported;

   C. the transaction exceeds withdrawal or purchase limits as may be applied by Issuers;

   D. a Permanent Decline or;

ix. ensure that any of the Acquirer' s Merchants or Service Providers do not attempt to reprocess an eftpos In-App Payment, where it exceeds any withdrawal or purchase frequency limits, which the Merchant and eftpos Consumer mutually agreed to in a Payment Arrangement; and

x. Other than in accordance with (viii) above, a Merchant may resubmit that transaction, no more than once per Calendar Day, up to a maximum of 4 retries over a period of 16 Calendar Days from the original declined transaction date.

4.7.12 Criteria for eftpos Open Loop Transit

eftpos Open Loop Transit capability allows Transit Scheme Operators and Transit Service Providers that form part of a Transit Scheme, to have eftpos Open Loop Transit transactions performed at their eftpos Terminals, by eftpos Consumers.

4.7.12.1 Minimum qualification criteria for eftpos open Loop Transit

a. An Acquirer must ensure that a Merchant processing eftpos Open Loop Transit transactions meets the minimum requirements set out in this section, in addition to the criteria in clause 4.7.5:

b. must be a Transit Scheme Operator; or

c. must be a Transit Service Provider; and

d. must be assigned by their Acquirer, an eligible Merchant Category Code of as defined in the OLT Acquirer Implementation Guide.

4.7.12.2 When Acquirers cannot offer eftpos Open Loop Transit

Acquirers cannot provide eftpos Open Loop Transit services to Merchants that do not meet the criteria set out in clause 4.7.12.1.

4.7.12.3 Minimum terms – eftpos Open Loop Transit

Acquirers of Merchants providing eftpos Open Loop Transit services must ensure that the Merchant:

a. enables eftpos Open Loop Transit for all eftpos Form Factors (for BIN ranges allowed by eftpos for use for a Transit Scheme), not on the Merchant's Deny List;

b. provides a technical solution that meets the requirements of sub-section 4.7.12.4 below;

c. complies with PCI DSS requirements in respect of any systems or process that stores or accesses Card numbers;

d. acknowledges that an Account Verify message for eftpos Open Loop Transit does not reserve any funds in a Cardholder's account and does not guarantee that any subsequent aggregated Purchase transaction will be approved;

e. acknowledges that the Merchant is responsible for the value of any travel initiated and permitted by the Merchant to continue using an eftpos Form Factor if the eftpos Form Factor is on a Deny List or an Account Verify message or Purchase is declined;

f. acknowledges that the Merchant is responsible for ensuring that each Purchase transaction represents accurate charges for the travel undertaken in accordance with requirements of Law;

g. establishes and is responsible for maintaining and updating a Deny List within 60 minutes after an AVR / DCP fare purchase recovery transaction is declined;

h. maintains BINs for eftpos Form Factors as notified by the Company to the Acquirer for the purposes of eftpos Open Loop Transit;

i. maintains Deny List for PANs and device PANs/tokens for eftpos Form Factors declined either for an Account Verify message or for a Deferred Card Present Purchase eftpos Transaction;

j. does not process a Deferred Card Present transaction for an amount greater than $100;

k. does not process any Deferred Card Present Transactions for a PAN for which a Transaction has been declined, as a result of a Permanent Decline; and

l. does not process any eftpos Open Loop Transit transactions for an eftpos Form Factor on the Transit Scheme's Deny List, until the eftpos Form Factor is removed from the Deny List.

4.7.12.4 Minimum requirements – eftpos Open Loop Transit

Acquirers must ensure that Transit Scheme Operators:

a. process eftpos Open Loop Transit transactions in accordance with the:

   i. eftpos Chip and Contactless Reader Specification and related Transit Addendum; and

   ii. eftpos Chip and Contactless Terminal Application Specification and related Transit Addendum; and

   iii. eftpos Technical, Operational and Security Rules

b. at the time an eftpos Form Factor is tapped at an eftpos Terminal:

   i. perform Offline Data Authentication in accordance with the eftpos Chip and Contactless Terminal Application Specification, and

      A. validate the eftpos Form Factor expiry date, to ensure the eftpos Form Factor has not expired; and

B. validate the eftpos Form Factor against the Transit Scheme Operator's Deny List;

C. validate the eftpos Form Factor for acceptable eftpos BIN range approved for use by a Transit Scheme.

ii. process an Account Verify transaction where the eftpos Form Factor has not been used:

A. for the Transit Scheme previously; or

B. for the Transit Scheme since last cut-off;

c. provide sufficient information within an eftpos Open Loop Transit transaction, to allow the transaction to be identified as an eftpos Open Loop Transit transaction processed through eftpos, on any transaction statement or record provided by the Merchant to the holder of the eftpos Form Factor;

d. maintain a current Deny List, which is deployed to the eftpos Terminals used as part of that Transit Scheme and updated, within 60 minutes after an AVR / DCP fare purchase recovery transaction is declined by the eftpos Issuer Member;

e. add an eftpos Form Factor to the Transit Scheme's Deny List after processing an eftpos Open Loop Transit transaction, with the outcome of either:

i. a declined Account Verify message, or

ii. after a declined eftpos Open Loop Transit Purchase transaction;

f. remove an eftpos Form Factor from the Transit Scheme's Deny List at the occurrence of:

i. Tap driven retry – where a Purchase transaction is generated and approved at the time the eftpos Form Factor is next presented at the eftpos Terminal;

ii. Scheduled retry – where a Purchase transaction is initiated by the Transit Scheme Operator periodically retrying that Purchase transaction to recover outstanding funds, no more than once per Calendar Day, up to a maximum of 8 retries over a period of 14 Calendar Days; or

iii. Customer service removal – where the eftpos Consumer contacts the Transit Scheme Operator and pays the amount of unpaid eftpos Open Loop Transit transactions, except where the Card had been added to the Deny List due to a Permanent Decline;

iv. an eftpos Form Factor can be removed only for temporary decline reason codes and not for a permanent decline reason code on Deny List.

g. generate a Purchase transaction for the aggregate value of the eftpos Open Loop Transit transactions for each eftpos Form Factor, no less than once per Calendar Day for the aggregate value / individual trip(s) of the eftpos Open Loop Transit transactions initiated on the immediately preceding Calendar Day;

h. respond to any Disputed Transaction in accordance with these Technical, Operational and Security Rules, the eftpos Disputed Transactions and Chargebacks Service Operations Guide, and the Transit Scheme's own terms and conditions;

i. manage any Sensitive Authentication Data in accordance with PCI DSS.

4.7.13 Criteria for eftpos QR (eQR) [Clause 4.7.13 is not applicable]

4.7.14 Payment Facilitators and Marketplaces

4.7.14.1 Minimum qualification criteria for Payment Facilitators and Marketplaces

a. An Acquirer may facilitate the provision of eftpos acceptance services to Merchants through Payment Facilitators and Marketplaces. In such instances the Payment Facilitator, the Marketplace and the End Merchant are Merchants for purposes of these Technical, Operational and Security Rules. As such, the provisions of clause 4.7 also apply to the Acquirer in respect of the Payment Facilitator and Marketplace as if it is the Merchant.

b. An Acquirer must ensure that it has an agreement in place with any Payment Facilitator and Marketplace which contains the minimum terms in clause 4.7.6 and clause 4.7.10 and must provide them with the operating guide that contains the matters set out in clause 4.7.3.

c. An Acquirer must satisfy itself that the Payment Facilitator and Marketplace:

   i. meets and demonstrates that they meet the requirements of any laws applicable to the nature of the business conducted by it;

   ii. demonstrates, to the Acquirer on enquiry, terms, conditions and policies that clearly articulate the customer enrolment, customer identification and verification checks on enrolment and throughout any Payment Arrangement period, credit limit setting, risk scoring and risk management, customer service and refunds policy, identification and qualification checks for participating End Merchants, clear End Merchant contract, documented End Merchant enrolment and education program, cancellation policy, and high levels of integrity in the application of their refund policy, past disputed transaction resolution and customer service;

   iii. must have, for at least 12 months unless otherwise notified by the Company, maintained acceptable fraud levels within the AusPayNet framework on a per calendar quarter basis, and must not have appeared on any payment network's non-compliance reporting – notification and/or enforcement;

   iv. must have maintained acceptable Chargeback levels within the requirements of clause 4.7.10.2 of these Technical, Operational and Security Rules;

v. demonstrates existing robust procedures relating to initial and ongoing Cardholder Authentication procedures, which meet the requirements of the CNP Standard, at the time of:

A. setting up an eftpos Consumer account;

B. enrolling an eftpos Consumer into a contracted service in respect of which eftpos Transactions will be initiated; or

C. expanding service offerings to an existing eftpos Consumer.

vi. demonstrates compliance and must maintain ongoing compliance with PCI DSS;

vii. displays the price for all eftpos Transactions to the eftpos Consumer at the time of Purchase and processing and, if necessary, refund in AUD;

viii. pays the full AUD amount for any refunded eftpos Transactions or any eftpos Transactions to which a Chargeback applies;

ix. only provides payment services to End Merchants that meet the MCCs and within the limits specified by the Company from time to time; and

x. shall format any eftpos Transaction processed by the Payment Facilitator for a Purchase or Refund on behalf of an End Merchant:

A. With the 'Merchant Name\Location' field identifying both the Payment Facilitator, and the End Merchant; The Payment Facilitator name to be in full or in abbreviated form. For clarity, it is not required to identify a physical location for the End Merchant in this field for eftpos Digital Acceptance and

B. With a Merchant Category Code set to the value defined within AS2805.16 which most accurately reflects the specific End Merchant providing goods or services to the cardholder.

xi. shall format any eftpos Transaction processed by the Marketplace for a Purchase or Refund

A. With the Marketplaces own MID, MCC, Name and Location; and

B. With a Merchant Category Code set to the value defined within AS2805.16 which most accurately reflects the specific goods or services provided to the cardholder.

d. An Acquirer must ensure that the Payment Facilitator is aware that the Payment Facilitator must not process transactions on behalf of another Payment Facilitator and must not be a Payment Facilitator for a Staged Digital Wallet.

e. If a Payment Facilitator is in breach of this clause, they may be suspended pursuant to clause 4.7.10.2.

f. If a Payment Facilitator operates as a Staged Digital Wallet Operator, the terms in 4.7.10.5 authorised Staged Digital Wallet operator minimum terms and 4.7.14.1 minimum qualification criteria for Payment Facilitators apply.

4.7.14.2 Suspension of Payment Facilitators and Marketplaces

An Acquirer must suspend a Payment Facilitator or Marketplace pending resolution in the following circumstances:

a. If the Payment Facilitator or Marketplace allows payments to be made to an End Merchant which provides goods or services of a nature that are, or would result in, a breach of laws.

b. If the Payment Facilitator is in breach of clause 4.7.14.1.e.

4.8. Devices running multiple applications

Where a device (e.g. PED) is running multiple applications, the SCD application and its associated data (including PINs and cryptographic keys) must be protected from any interference or corruption caused by any other application(s) and data.

4.9. TCP/IP Terminal connectivity

The following requirements apply to Acquirer's host systems which support Terminals using TCP/IP protocol for communications:

a. Stateful firewalls must protect all external entry points to the host environment;

b. Strong financial message protocol validation must be performed between eftpos Terminals and acquiring hosts;

c. Acquiring host must be located in a secure, protected network separate from generic internal and external access;

d. Security Control Modules must be accessible only to authorised hosts and authorised applications. Where connected via TCP/IP they must be on a separate, stand-alone network;

e. There shall be no uncontrolled connections between general internal and external networks and POS/SCM networks (assuming they are all TCP/IP);

f. The host environment shall provide, at a minimum, an IPS or IDS between the perimeter network firewall and the POS host;

g. The host system must provide appropriate threat management techniques relevant to the host's operating platform, such as malware protect with up-to-date signatures and maintenance, vulnerability patching, etc.;

h. All systems within the POS host environment must comply with all applicable requirements of PCI-DSS;

i. The host shall provide a mechanism for the rapid disablement of known/suspected compromised Terminals.

4.10. Customer interface at Terminals

Acquirers can adopt their own customer interface at Terminals, but that interface must be completely unambiguous, i.e. the meaning and intent of each instruction and prompt must be clear and convey only one meaning.

4.11. Record of Transaction

A Record of Transaction generated by a Terminal must be laid out in a clear manner, with all information shown in an unambiguous fashion. The information provided must comply, as a minimum, with the standards detailed in the ePayments Code.

The Record of Transaction may be provided to a consumer in a printed or electronic manner, subject to the conditions and disclosure requirements set out in the ePayments Code.

In addition to these requirements, any PAN or Payment Token included on the Record of Transactions must have at least four digits excluded. The preferred method of truncation is to print the first six digits and the last 3 digits of the PAN or Payment Token on the Record of Transaction. The card expiry date must be excluded from the Record of Transaction.

Where a transaction is declined by the card chip (offline decline), the Application Authentication Cryptogram (AAC) must also be printed on the receipt.

4.12. Acquirer requirements

4.12.1 Supported eftpos Form Factors

All approved eftpos Form Factors (including eftpos Cards) as defined in the Scheme Rules are to be supported by an Acquirer. All contact and contactless eftpos Terminals (including ATMs) must be capable of accepting eftpos Chip and Contactless (ACe).

4.12.2 Supported transactions

All eftpos Transactions

An Acquirer must be capable, as a minimum, of supporting the eftpos Transactions as defined in the Scheme Rules.

Prepaid Cards must not be used to perform Medicare Refund transactions.

eftpos Acquirers are required to send Track 2 Data in all financial transaction advice (0220) and Acquirer reversal advice (0420) transactions sent across the eftpos Hub for the eftpos Issuer BINs published by eftpos to Members from time to time.

Terminals

All eftpos Terminals must be upgraded and activated to accept the supported transaction set as initiated by eftpos Chip and Contactless (ACe) enabled Cards as defined in eftpos Terminal Application Specifications.

The transaction types supported for eftpos Terminals must be processed in accordance with the eLS.

All Acquirers Terminals must be capable of initialising the supported transaction set through a contact or contactless chip reader. In addition, dual interface and contact-only Terminals shall incorporate a magnetic stripe reader. Note that the requirement for a magnetic stripe reader does not apply to mPOS-SPoC acceptance devices.

The supported transaction set must be capable of being initiated by eftpos Chip and Contactless (ACe) enabled Multi-Network Cards.

The supported transaction set must be capable of being initiated by eftpos Chip and Contactless (ACe) enabled Issuer proprietary cards.

The supported transaction set may be capable of being initiated by eftpos Chip and Contactless (ACe) enabled reloadable Prepaid Cards.

The presence of MCR tag is mandatory in the transaction messages sent from Acquirers to the eftpos Hub for any eftpos Transactions if a Merchant exercises its right to choose an eftpos application present and available for selection on the Multi-Network Debit Card to complete a contactless transaction. This requirement does not apply to:

a. contact transactions, even if initiated using a Multi-Network Debit Card; or

b. contactless transactions initiated using Multi-Network Credit Cards, eftpos Proprietary cards, ACe enabled reloadable Prepaid Cards.

Cashout

The Company, from time to time, may not require Cashout to be supported on certain Acceptance Devices.

If the eftpos Terminal being certified is deployed in multiple Merchants' environments and at least one of the Merchants supports Cashout, Acquirers must certify the Terminal for Cashout. It would then be at the individual Merchant's discretion to support Cashout.

Otherwise, if the Terminals will be deployed only to Merchants/Merchant types (e.g. Taxis) that don't offer Cashout because this is not part of their business model, then certification of Cashout becomes optional.

eftpos Form Factors provisioned for use in eftpos Mobile

Acquirers must support acceptance by their Merchants of eftpos Transactions initiated by an eftpos Form Factor enabled for eftpos Mobile for using compatible Mobile Devices as published by the Company from time to time in the eftpos Mobile Member Implementation Guide. Acquirers must route transactions according to the Payment Token BINs published by eftpos to Members from time to time.

Acquirers must support ATM balance enquiries using an eftpos Form Factor enabled for eftpos Mobile for any ATMs deployed by those Acquirers or where the Acquirer is a Clearing Agent or Processor for a Member that deploys ATMs.

eftpos In-App Payments

Acquirers supporting eftpos In-App Payment capability must obtain certification for In-App Payments messages passing between the Acquirer and eftpos Hub relating to eftpos In-App transactions initiated through eftpos Mobile.

The following Transaction types are supported for eftpos In-App Payments and must be processed in accordance with the eLS:

a. Purchase

b. Refund:

   i. for transactions where Payment Token credentials are available; and

   ii. for transactions where no Payment Token credentials are available, using the Card details provided by the eftpos Consumer at the time of processing the refund transaction.

c. Account Verify

eftpos In-App Payments are considered to be eftpos Form Factor Present Transactions.

By 1 May 2022, Acquirers are required to support In-App Payments for device associated eftpos Payment Tokens for Multi-Network Debit cards provisioned to an OEM Solution.

eftpos Digital Acceptance

An Acquirer or Self-Acquirer can only implement eftpos Digital Acceptance using a service that meets the eftpos CNP Standard. An Acquirer or Self-Acquirer can only offer eftpos Digital Acceptance to Merchants that meet the requirements of 4.7.5 and 4.7.10.1.

Participating Member Acquirers must or must require the Merchant Service Provider to support the following transactions:

a. No longer used;

b. eftpos eCommerce Purchase transaction (0200);

c. eftpos Refund transaction (0200);

d. No longer used;

e. No longer used;

f. the reversal of an eftpos Transaction (0420); and

g. The Company may set and notify Members of maximum limits for Deposit Transactions from time to time.

By 1 May 2022, Acquirers are required to implement functionality to support processing of CNP Purchase and Refund transactions. Acquirers may comply by supporting eftpos CNP payment messages via Switch to Acquirer (S2A) or Switch to Issuer (S2I) processing models. Switch to Issuer is where a transaction is routed directly to the Issuer for authorisation. This model is in use for Gateways as Direct Connectors to the eftpos Hub.

The eftpos Fast Notification Payment Advice solution is a service that an eftpos Acquirer Member may subscribe to when that Acquirer supports Gateways routing payment transactions under the eftpos Switch to Issuer (S2I) solution. Please refer to S2I Implementation guide for details on S2I service. Please refer to S2I Implementation guide for details on S2I service.

Acquirers must not onboard and process CNP Purchase or Refund transactions from Merchants classified as Extreme Risk as defined within eftpos CNP Standard.

eftpos Digital Acceptance must not be used for:

a. Cashout;

b. Mail Order/ Telephone Order (MOTO) transactions where new PAN details are required (for clarity this does not apply to existing COF transactions);

c. transaction types as defined in Scheme Rule 22.2(a) (ii), (iii) and (v).

Participating Acquirers must provide eftpos Digital Acceptance payment acceptance choice to their Authorised eftpos Digital Merchants that meet the requirements set out in these Technical, Operational and Security Rules. If a Participating Acquirer provides eftpos Digital Acceptance payment acceptance services to Merchants for any payment system and the Merchant meets the requirements set out in these Technical, Operational and Security Rules, in addition to the requirements of Scheme Rule 23, the Acquirer must:

a. provide eftpos Digital Acceptance payment acceptance choice; and

b. ensure, where an Authorised eftpos Digital Merchant allows eftpos Consumers to choose processing via eftpos Digital Acceptance, the Authorised eftpos Digital Merchant provides the ability for eftpos Consumers to change the default or priority payment system selection to enable eftpos Digital Acceptance to be selected as the eftpos Consumer's default or primary payment choice on a per transaction or account settings basis;

Prepaid Cards must not be used to perform eftpos Transactions using eftpos Digital Acceptance (other than eftpos Mobile), except where authorised by Issuer and the Company.

eftpos Open Loop Transit

a. Any Acquirer of eftpos Open Loop Transit, must enable all holders of an eftpos Form Factor to initiate an eftpos Open Loop Transit transaction.

b. The following Transaction types are supported for eftpos Open Loop Transit and must be processed in accordance with the eLS:

c. Account Verify;

d. Deferred Card Present Purchase.

e. Account Verify and fare recovery Purchase transactions are processed as Deferred Card Present Transactions.

eftpos QR payments

Note: That the clause below relating to eQR has not been ratified and is not yet applicable to Members

a. eQR transactions may be considered eQR authenticated or eQR unauthenticated transactions.

   i. eQR authenticated transactions - eQR Pass Through Wallet transactions and transactions authenticated through eftpos Secure ~~where the authentication was performed during the payment~~ are considered eQR authenticated transactions.

   ii. eQR unauthenticated transactions- eQR transactions which are not considered eQR Pass Through Wallet transactions or have not been authenticated through eftpos Secure

b. The following Transaction types are supported for eQR transactions and must be processed in accordance with the eLS:

   i. Purchase Transaction

   ii. Refund Transactions: and

   iii. Reversals of these transactions

c. Acquirers must support acceptance of eQR Transactions by their Merchants as defined by the Company from time to the eQR Acquirer Implementation Guide and eQR Merchant Enablement Guide.

   i. eQR CNP transactions utilising existing eftpos CNP standard and eftpos Secure can be used for only online transactions if eQR Pass Through Wallet capability is not available.

   ii. Refer to eLS for relevant data fields

   iii. eQR unauthenticated transactions are allowed only for merchants defined under low risk of fraud. (Refer to advice: no QR Code fraud shift)

The full PAN must not be displayed as part of the user display on the third party wallet to which an eftpos Form Factor is provisioned unless the eftpos Consumer has unlocked their application in the third party wallet. The use of a Masked PAN where either the first 6 and last 4 digits or just the last 4 digits of a PAN are displayed is permitted.

By 1 May 2023, all new (non-legacy) Terminals installed from this date must support eQR Code presentation to Consumers.

By 1 May 2024, all (non-legacy*) Terminals must support QR Code presentation to consumers. (Refer to eQR Merchant Enablement Guide for details)

4.12.3 Card Authentication Method (CAM) [Clause 4.12.3 is confidential]

4.12.4 Cardholder Verification Method (CVM)

PIN Bypass is not supported, and Acquirers must support the following CVMs

4.12.4.1 Online PIN

The Use of Online PIN authentication must be supported for all Transactions unless the Transaction is a:

a. Chip Fallback

b. Electronic Fallback

c. Manually entered transaction

d. Contactless purchase under the card’s CVM limit

~~e.~~ eftpos Mobile transaction under the Form Factor CVM limit.

For clarity the use of Online PIN for Refund Transactions is optional.

4.12.4.2 Consumer Device Cardholder Verification Method (CDCVM)

CDCVM is used where an eftpos Consumer using an eftpos Form Factor in a Mobile Wallet or OEM Solution, performs an eftpos Transaction above the CVM limit by the eftpos Issuer, and/or is otherwise required to verify themselves directly onto the Mobile Device used to perform the transaction in accordance with the eftpos Mobile Member Implementation Guide. CDCVM may also be used outside of transaction processing, to identify an eftpos Consumer.

CDCVM must be supported on Acceptance Devices certified on the eftpos Terminal Application Specification v16.02 or later and activated on deployment. Until the Acceptance Device supports CDCVM, the eftpos Consumer will be prompted to enter their PIN onto the Acceptance Device.

For the purposes of Section 7 of these Technical, Operational and Security Rules, transactions using a CDCVM are treated as Form Factor present transactions.

4.12.4.3 No longer used

4.12.4.4 Offline PIN

The use of Offline PIN authentication must be supported when directed to do so by the eftpos Form Factor.

4.12.4.5 Signature

A signature CVM is only used for transactions that qualify for Electronic Fallback or key entered processing.

4.12.5 No CVM [Clause 4.12.5 is confidential]

4.12.6 CVM limits for Contactless

The CVM limit on a contactless Form Factor, including eftpos Form Factors enabled for use in a Mobile Wallet utilising eftpos Mobile functionality is determined by the Issuer, unless the transaction has a cash component in which case the CVM limit is zero.

Transactions on a contactless eftpos Form Factor in excess of the Issuer defined CVM limit require the eftpos Form Factor PIN or other authentication method approved by the Company to be input into the Acceptance Device.

4.12.7 Chip and Contactless scripting

When received, Acquirers must pass Issuer scripts to the card.

4.12.8 Account selection

At a minimum, an Acquirer must provide for account selection of both eftpos Savings and Cheque at eftpos Terminals.

For eftpos Digital Acceptance, Acquirers must ensure that their Authorised eftpos Digital Merchants do not require account level selection on the checkout screen.

4.12.9 Medicare Claim refunds

Prior to the notification by the Company of the implementation of the eftpos Deposit transaction in the Card Present environment for Medicare, an Acquirer that initiates a Refund Transaction to make a Medicare Claim Refund must populate Field 43 of the applicable 0200 or 0220 message with only the words “Medicare Benefit”.

4.12.10 PIN data

Where a transaction contains PIN data (Field 52), that PIN data must be formatted in accordance with one of PIN Block formats specified in AS 2805 part 3 with the exception of formats 1, 2 and 8. Transactions containing a zero length PIN (format 8) are not to be propagated through Interchange but rather terminated at the Terminal or Acquirer host.

4.12.11 Privacy of communication for all Terminal to Acquirer links

This clause applies to links between an eftpos Terminal and Acquirer.

Acquirers must ensure that privacy of communication complies with AS 2805 part 9, or any other privacy of communication standard approved by the Company.

4.12.11.1 Terminal and host requirements for Pre-Authorised Transactions

Terminals and Acquirer host systems supporting the Short-duration Pre-Authorised Transaction must be designed to ensure that the financial transaction advice message (message type 0220) that concludes the Pre-Authorised Transaction is sent on-line immediately upon the conclusion of the transaction and not stored within the Terminal or Acquirer host for later batch transmission to the Issuer.

Where a Merchant or Acquirer pre-set upper limit is used for the financial transaction request message Merchants must ensure that the cardholder is appropriately informed of this action especially where an "insufficient funds" response is returned to the financial transaction request message.

4.12.12 No longer used

.

4.13. User Experience

Acquirers must ensure interoperability of eftpos Form Factors accepted through Acceptance Devices for which they are a Clearing Agent.

Acquirers must ensure that an eftpos Consumer using an eftpos Terminal is only required to tap an eftpos Form Factor once to initiate and confirm each eftpos Transaction.

4.14. Enquiries

4.14.1 Cardholder enquiries

Acquirers receiving enquiries directly from Cardholders concerning eftpos Transactions are to refer the Cardholders to their Issuer.

Cardholders should not be referred back to the initiating Merchant except in the case of enquiries relating to the supply or quality of goods or services purchased through an eftpos Transaction.

4.14.2 Merchant enquiries

Acquirers must require Merchants to refer any queries regarding eftpos Transactions to the Acquirer's help desk and not directly to the Issuer.

4.14.3 Branch enquiries

Members are to direct all enquiries from their branch network to their own eftpos operations area and not directly to other Members or to another Member's Merchant.

4.15. Cards left on Merchant's premises

If a Card is accidentally left behind on a Merchant's premises, the Acquirer procedures must require the Merchant to:

a. retain the Card in a secure place for a period of up to two business days; and

b. hand the Card to the claimant only after having established the claimant's identity by comparing signatures; or

c. hand or return the Card to the Acquirer via a secure method if not claimed within two days.

The Acquirer is to forward the Card to the Issuer via a secure method at earliest opportunity. Issuer contact details are found on the Australian Payments Network Extranet at https://extranet.auspaynet.com.au/.

4.16. Compromised Terminals [Clause 4.16 is confidential]

4.17. Fraud monitoring program

The eftpos Fraud monitoring program defines acceptable tolerances for Fraud volumes under which Issuers and Acquirers must operate. Warning and breach thresholds for the program are closely aligned to the AusPayNet CNP Fraud Framework.

Each quarter (calendar quarter), the Company will make available to each Acquirer Member, a quarterly fraud reporting dashboard and portfolio quality report which outlines their performance to the program. Members who breach these programs will be required to provide the Company a Member action plan at both the warning threshold and breach threshold outlining actions being taken to bring fraud basis points below the threshold. Acquirer Members are required to submit action plans within one (1) calendar month of receiving the breach notification from eftpos.

These actions plans shall be submitted via email to: fraud@auspayplus.com.au.

The program is set out below, and further requirements are referenced within the eftpos Fraud Operations Guide.

Any Merchant	Warning threshold	Breach threshold
Approved fraud breach amount threshold (in-scope CNP transactions)	**20bps** or greater and **$50k** or greater of Fraud	**20bps** or greater and **$50k or** greater of Fraud
Breach period consecutive quarters	2	3
Measurement method	Member Fraud Reporting Dashboards and portfolio quality report.	Member Fraud Reporting Dashboards and portfolio quality report
Member requirement	• Completion of Member Action Plan Template when in breach of warning threshold. • Provision of Australian Payments Network Merchant Breach Report • Leveraging eftpos fraud scoring	• Completion of Member Action Plan Template when in breach of warning threshold • Provision of Australian Payments Network Merchant Breach Report • Leveraging eftpos fraud scoring
Consequence		Breach notification and fine decision as set out in the Scheme Rules – Part D Clause 16 Fines.

5. Security

5.1. Prevention of unauthorised access

All Members shall maintain procedures for avoiding any unauthorised access to. or use of, the Interchange system through its own hardware, software, Interchange Lines which enable the exchange of authorisation and reconciliation of Transactions.

All Members and eftpos shall maintain procedures for avoiding any unauthorised access to, or use of, the API connection through its own hardware, software, Interchange Lines which enable the exchange of API's.

5.2. Interchange of cryptographic keys

Interchange keys are used to protect financial transactions initiated at Acquirer eftpos Terminals while in transit to the Issuer institution. Interchange keys may be either:

a. PIN encrypting keys – used to protect the customer PIN from the point of origin to the point of authorisation. PIN encrypting keys are a specific instance of session keys;

b. Session keys – used to secure, validate and protect the financial message. Session keys can be further qualified into those used in the Terminal to Acquirer environment (Terminal session keys) or on node to node links (interchange session keys);

c. Key Encrypting Keys (KEK) – used to protect other keys (e.g. session keys) during exchange; or

d. Transport Keys – used to protect keys (e.g. KEKs) during transport to the partner institution.

e. Mutual SSL – used for API Gateway. Details provided in API Gateway Services Schedule.

5.3. Cryptographic algorithms

DEA3 and DEA2 are the only approved algorithms for the protection of interchange information (full details of these algorithms may be found in the Australian standard AS 2805 Part 5).

DEA3 keys are 128 bits in length (effectively 112 bits) and are generally referred to as Triple DES or 3DES keys (the corresponding encryption algorithm is specified in AS 2805 Part 5.4). Triple DES may also be acceptably implemented using a key length of 192 bits (effectively 168 bits).

DEA3 with a key length of 128 bits and DEA2 with key lengths equal to, or greater than 2048 bits are the minimum acceptable requirements for the effective protection of interchange information at the time of the issuance of this document.

In accordance with AS 2805 Part 3, DEA3 must be used for PIN encipherment.

5.4. Interchange links

For all Interchange Links, Issuers and Acquirers must ensure that:

a. Security for Transactions processed over that Interchange Link complies with AS2805 Part 6;

b. Message formats comply with AS2805 Part 2;

c. Security of transactions from Terminal to Acquirer and from Acquirer to Issuer complies with AS2805 Part 6;

d. PIN security and encryption complies with AS2805 Parts 3 and 5.4;

e. Key management practices comply with AS2805 Part 6.1;

In each case and as more particularly set out in Part 6:

a. Message Authentication must apply to all Interchange Links;

b. The Message Authentication Code (MAC) must be calculated using, as a minimum, a DEA 3 (128-bit) key, Triple DES and an algorithm conforming to AS2805 Part 4; and

c. All interchange PIN and MAC cryptographic functions must be performed within a Tamper-responsive SCM.

d. For connectivity to eftpos API Gateway, Members / Direct connectors must ensure that:

e. Security of the API's processed over the link complies with eftpos security requirements specified in eftpos API Gateway Services Schedule

f. Message formats comply with eftpos API specifications.

5.4.1 Key management practices – Interchange links [Clause 5.4.1 is confidential]

5.4.2 Key rolling process for Interchange Key Encrypting Keys (KEKs)

The procedure to be adopted for the exchange of Interchange Key Encrypting Keys (KEKs) are detailed in Section 6.6.2.

5.5. Interchange Lines

Interchange Lines shall be subject to whole-of-message encryption, excluding communications headers, using at a minimum Tripe DES and a DEA 3 (128 bit) – bit key in accordance with AS 2805 Part 5.4.

5.5.1 Interchange Line cryptographic management

Subject to Clause 5.4.2, the use of transport level data encryption (e.g. IPSec) is permitted subject to the following conditions:

a. data encryption must use Triple DES with either a 128-bit or 192-bit key length;

b. the data stream must be fully encrypted with the exception of communication headers;

c. either certificates or encrypted pre-shared secrets must be used (plain text shared secrets are not acceptable);

d. tunnel termination points must be within the Member's or their trusted agent's facilities;

e. the facility must be supported by documented device management procedures with identified roles and responsibilities and subject to internal audit as prescribed by the Member's security policy;

f. ownership and control of end-points must reside with the terminating Member;

g. split tunnelling is not to be used; and

h. the minimum Diffie-Hellman MODP group size is 1536-bits.

Where encrypted shared-secrets are used, key management, including the process of key (secret) entry must comply with the requirements of AS2805 Part 6.1, especially the requirement that no one person shall have the capability to access or ascertain any plain text secret or private key.

Manual key change is not permitted. Automated key change through router configuration is permitted.

5.5.2 Key management practices for Interchange Lines [Clause 5.5.2 is confidential].

5.6. Cryptographic key management – general

Unless specifically detailed elsewhere, the following key management practices shall apply. All cryptographic key management practices shall conform to AS 2805 Part 6.1.

5.6.1 Transport Keys

5.6.1.1 Approved encyrption algorithms for Transport Keys

DEA2 and DEA3 are the only approved algorithms for the protection of keys in transport.

Direct Connectors through a Standard Hub Service must comply with the COIN Operating Manual in respect of approved encryption algorithms for transport keys.

5.6.1.2 Minimum key length for Transport Keys

DEA2 keys of less than 2048 bits are to be treated as single use keys and their use is deprecated.

DEA 2 key lengths of less than 1024-bits are unsuitable for general use. Preferred DEA2 key lengths are equal to or greater than 2048 bits in length and should be used in all new implementations where hardware constraints do not exist.

Triple DES (DEA 3) may use either 128-bit or 192-bit key sizes.

Direct Connectors through a Standard Hub Service must comply with the COIN Operating Manual in respect of key length for transport keys.

5.6.1.3 Key lifecycle practices for Transport Keys

DEA 3 Key Transport Keys are single use keys only.

They must be freshly generated to protect keys in transport and then securely destroyed after use.

At the time of publication, DEA 2 keys of size equal to or in excess of 2048 bits are deemed acceptable for a key change interval (lifetime) of two (2) years.

5.6.2 Domain Master Keys (DMKs)

These keys are used within a financial institution to protect keys stored internal to the organisation.

5.6.2.1 Minimum key length for Domain Master Keys

Domain Master Keys shall be DEA 3 keys with a minimum length of 128-bits (112 effective).

5.6.3 Issuer Master Keys (IMKs)

Requirements relating to the IMK set are detailed in the eftpos Card Application Personalisation Specification.

5.6.4 Issuer Public Keys (IPKs)

Compliance requirements for Issuer Public Key lengths and expiry dates are published from time to time by the company with reference to EMVCo guidelines.

5.7. Tokens [Clause 5.7 is confidential]

6. Infrastructure

6.1. Purpose

The purpose of this Part 6 is to provide an overview of the standard message set capable of supporting the range of eftpos Transactions arising from eftpos only eftpos Form Factors or Multi-Network Cards through approved channels.

The detailed requirements for Direct Connections to:

a. the eftpos Hub are specified in the eftpos Hub Link Specification and are supported by the Standard Hub Service Schedule;

b. the eftpos TSP are specified in the eftpos Hub Link Specification, API Specification and are supported by the eTS-F Service Schedule;

c. the eftpos API Gateway are specified in the eftpos API Specifications and are supported by the eftpos API Gateway Services Schedule.

d. the eftpos Secure Directory Server are specified in the eftpos Secure Specifications and are supported by the eftpos Secure Service Schedule

6.2. Scope

The scope of this Part 6 is to outline:

a. the eftpos Transaction types and message types for processing of eftpos Transactions across Interchange Links to the eftpos Hub.

b. The requirements of these Technical, Operational and Security Rules and the eftpos Hub Link Specification take precedence over those of the AS2805 standard if any contention arises during the implementation of an interface using this specification.

c. the eftpos Transaction types and message types for detokenizing Payment Tokens before processing of eftpos Transactions via the eftpos Hub.

6.3. Supported message types

This section applies to eftpos Hub Direct Connections. The supported message types relating to eftpos Hub processing are set out below and detailed in the eftpos Hub Link Specification. Supported message types for an eftpos Mobile Solution and eTS-F are detailed within the relevant eLS Token Management

Addendum. Supported message types for eftpos Secure are detailed within eftpos Secure Specifications.

Request	Response	Message types
0100	0110	Account Verify Request
0200	0210	Financial Transaction Request
0220	0230	Financial Transaction Advice
0221	0230	Financial Transaction Advice Repeat
0420	0430	Acquirer Reversal Advice
0421	0430	Acquirer Reversal Advice Repeat
0520	0530	Acquirer Reconciliation Advice
0521	0530	Acquirer Reconciliation Advice Repeat
0800	0810	Network Management Request
0820	0830	Network Management Advice

Table 4: Supported message types

6.4. Supported Transaction set

This section applies to eftpos Hub Direct Connections as far as being a statement of supported transactions. The eftpos Hub Link Specification details the requirements and the process.

6.4.1 Account Verify transactions

For eftpos Digital Acceptance, Participating Member Acquirers may initiate an Account Verify (0100) transaction, whether or not at the time an order for goods or services is processed.

For eftpos Open Loop Transit, Participating Member Acquirers may initiate an Account Verify (0100) transaction where an eftpos Form Factor has not been presented for an eftpos Open Loop Transit transaction previously or within a period defined by the Transit Scheme Operator.

Member Issuers must be capable of responding to an Account Verify 0100 message in accordance with the eftpos Hub Link Specification.

6.4.2 Pre-Authorised transactions

Short Duration Pre-Authorised Transactions

A Short Duration Pre-Authorised transaction is a two-phase transaction. A Financial Transaction request (message type 0200) is used by the card acceptor as a guarantee of funds from the card Issuer or their agent. This message is followed by a reversal (message type 0420), on sale completion, for the full amount of the 0200 and the transaction concluded by a Financial Transaction Advice (message type 0220) for the actual amount of the sale. The authorisation received for the 0200 is deemed to apply to the 0220 provided the 0220 is less than or equal to the 0200.

Under no circumstances should the amount of the financial transaction advice message exceed the value of the financial transaction request message. Where this occurs the Acquirer shall be liable for any amount in excess of the authorised value. As liability can be facilitated by the presence of DE 90 (refer clause 2.12), Acquirers must provide DE90 to avoid unnecessary disputes and chargebacks.

Where the 0200 is equal to the actual amount of the sale, a reversal (0420) in conjunction with an advice (0220) are optional.

For the purposes of the eftpos Hub Link Specification, these transactions are referred to as purchase/reversal/advice transactions.

Short Duration Pre-Authorised transactions are not to be used where the total lifetime of the transaction, that is the time from the financial transaction request message to the submission of the final transaction request advice message, exceeds fifteen minutes.

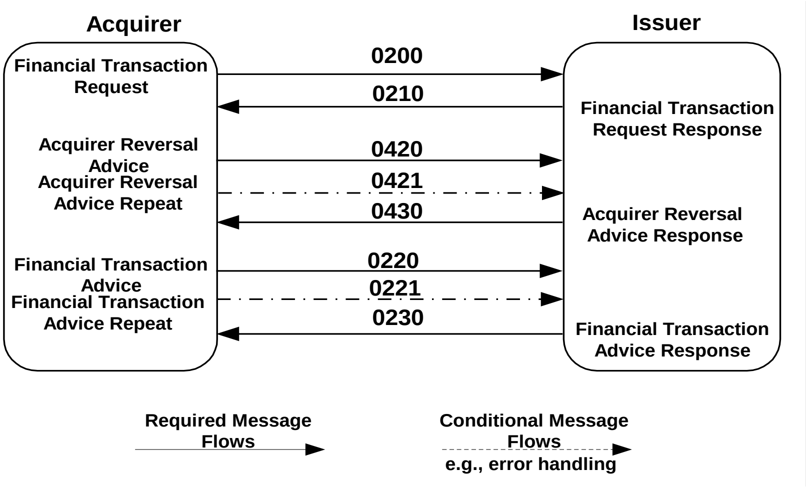

Acquirer
Issuer
Financial Transaction Request
Acquirer Reversal Advice
Acquirer Reversal Advice Repeat
Financial Transaction Advice
Financial Transaction Advice Repeat
0200
0210
0420
0421
0430
0220
0221
0230
Financial Transaction Request Response
Acquirer Reversal Advice Response
Financial Transaction Advice Response
Required Message Flows
Conditional Message Flows
e.g., error handling

Figure 1: Short Duration Pre-Authorisation transaction flow

Short Duration Pre-Authorised transactions are generated from devices such as fuel dispensers, taxis and card-activated phones. The transaction is used where the Merchant or Terminaldoes not know the final cost of the goods or services to be provided. The financial transaction request message will contain either a Merchant/Acquirer specified default maximum amount or a cardholder specified maximum at the Acquirer's discretion.

The Financial Transaction Advice that completes the transaction must be for a value equal to or lower than the amount for which the financial transaction request was approved.

Short duration Pre-Authorised financial transaction advice messages may be identified by the presence of data element 90 in conjunction with data element 25 values of 42 or 43 (electronic payment Terminal/Card activated fuel dispenser) or to differentiate fallback related financial transaction advice messages by the absence of any fallback indicator ("FBxx\") in Data element 47.

6.4.3 Purchase Transaction

A Purchase Transaction is used by an Acquirer to request authorisation from the Issuer of a card, to complete a Cardholder initiated purchase transaction with a Merchant or service provider.

Acquirer Reversal Advice (0420) messages are used to handle error conditions arising from the inability to complete the transaction.

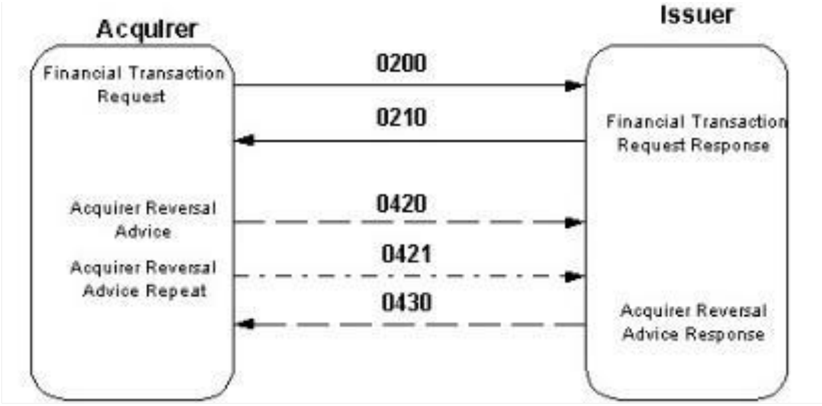

Acquirer
Issuer
Financial Transaction Request
0200
0210
Financial Transaction Request Response
Acquirer Reversal Advice
0420
Acquirer Reversal Advice Repeat
0421
0430
Acquirer Reversal Advice Response

Figure 2: Purchase Transaction flow

6.4.4 Cashout Transaction

A Cashout transaction is used by an Acquirer to request authorisation from the card Issuer to complete a Cardholder initiated Cashout request at an eftpos Terminal. Cashout transactions must be legal tender amounts and the currency provided directly to the cardholder in the form of cash, this being with Australian notes or Australian coins.

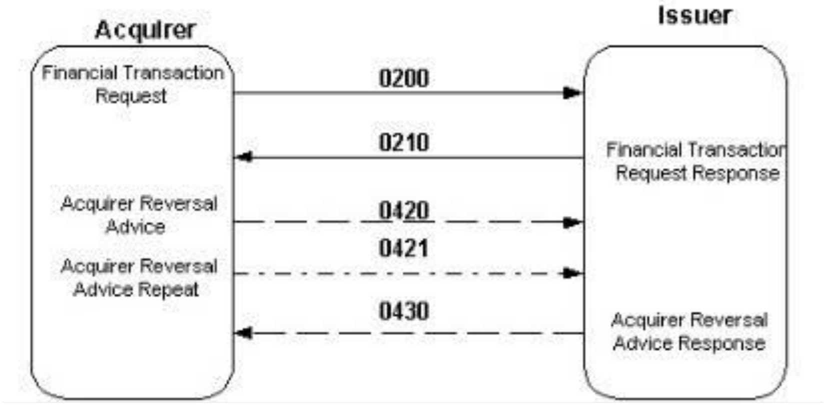

Acquirer
Issuer
Financial Transaction Request
0200
0210
Financial Transaction Request Response
Acquirer Reversal Advice
0420
Acquirer Reversal Advice Repeat
0421
0430
Acquirer Reversal Advice Response

Figure 3: Cashout Transaction flow

6.4.5 Combined Purchase and Cashout Transaction

A combined Purchase and Cashout Transaction is an eftpos-only transaction where the Cardholder is supplied with some goods and/or services and at the same time with Cash funds. The Cash component must be a legal tender amount and the currency provided directly to the cardholder in the form of cash, this being with Australian notes or Australian coins.

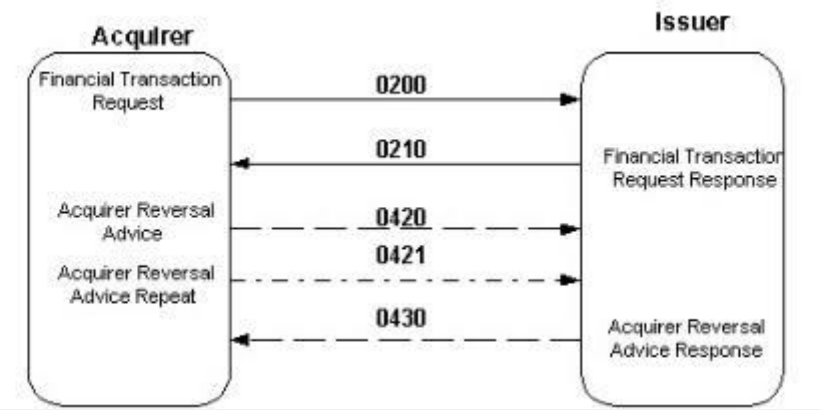

Acquirer
Issuer
Financial Transaction Request
0200
0210
Financial Transaction Request Response
Acquirer Reversal Advice
0420
0421
Acquirer Reversal Advice Repeat
0430
Acquirer Reversal Advice Response

Figure 4: Combined Purchase and Cashout Transaction flow

6.4.6 Fallback Transaction

Fallback Transactions are used when there is a failure to process an eftpos transaction on line. The failure could be at the Merchant's device, the Merchant to Acquirer link or the Interchange. Fallback Transactions can only be used in the case of specific failures as detailed in Section 2.12.1

There are 2 permitted fallback modes for ICC originated transactions:

a. Chip Fallback: occurs where the transaction rules require online authorisation and the Terminal is unable to go online. Transaction processing proceeds in accordance with the card's Chip Fallback limits.

b. Technology Fallback: occurs when due to a fault of either the ICC or the IFD, the Terminal is unable to retrieve data from the chip. Fallback is to magnetic-stripe.

c. Chip Decision Override (CDO or Fallback Override) refers to the situation where, in Chip Fallback, the ICC returns a decline, and where the Merchant chooses to override the result. CDO is not permitted unless mutually agreed between parties.

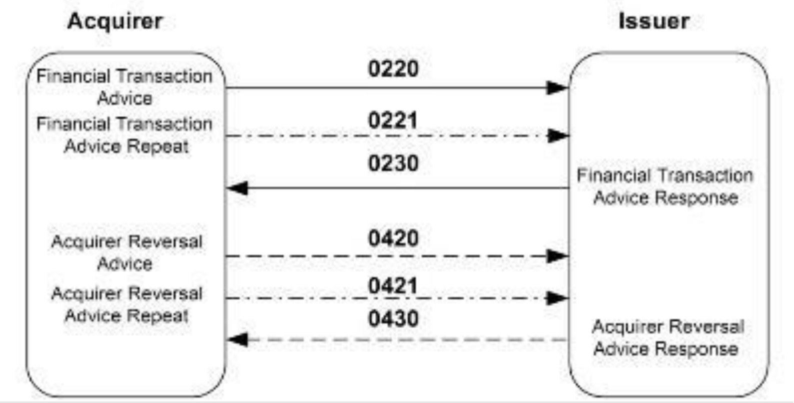

Acquirer
Issuer
Financial Transaction Advice
Financial Transaction Advice Repeat
0220
0221
0230
Financial Transaction Advice Response
Acquirer Reversal Advice
Acquirer Reversal Advice Repeat
0420
0421
0430
Acquirer Reversal Advice Response

Figure 5: Fallback transaction flow

A repeat advice message (0221) may be sent when the Terminal fails to receive a 0230 Financial Transaction Advice response or when the Terminal fails to authenticate the 0230 response message.

6.4.7 Refund Transaction

A Refund Transaction is initiated when a Merchant or Service Provider has a need to return funds to a Cardholder in respect of a prior purchase, for example, if the Cardholder has returned unwanted goods.

Prior to the date Deposit transactions are supported through all transaction channels, a refund Transaction may also be initiated when a Merchant or service provider has a need to:

a. pay funds to a Cardholder in circumstances that the Issuer and the Acquirer have bilaterally agreed; or

b. make a Medicare Claim Refund.

From the date Deposit transactions are supported through all transaction channels, the refund Transaction is only to be used to return funds to a Cardholder in respect of a prior purchase and the Deposit Transaction must be used for any other transfer of funds to a Cardholder.

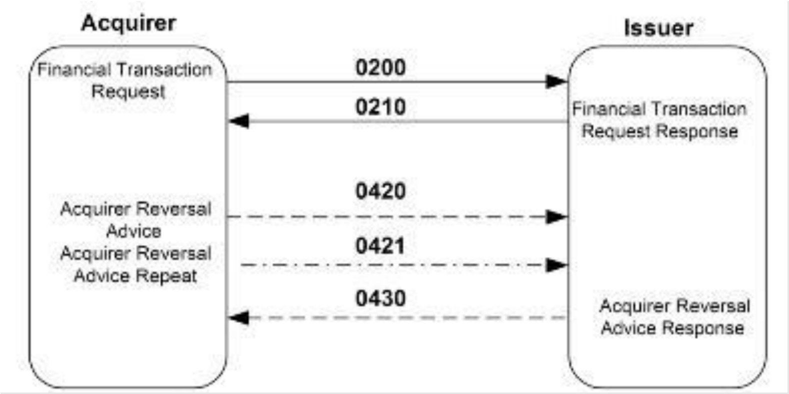

Acquirer
Issuer
Financial Transaction Request
0200
0210
Financial Transaction Request Response
0420
Acquirer Reversal Advice
Acquirer Reversal Advice Repeat
0421
0430
Acquirer Reversal Advice Response

Figure 6: Refund Transaction flow

eftpos Refund Transactions are processed as EMV downgrade transactions, with PIN verification optional. It is the decision of the Acquirer to determine whether a Terminal prompts for CVM.

Issuers must be able to support a downgraded Refund transaction with the following POS Entry Modes populated in Field 022 of the Financial Transaction Request Message in accordance with the eftpos Hub Link Specification (eLS):

a. 021 Mag stripe;

b. 051 contact ICC; and

c. 071 contactless ICC

6.4.8 Deposit Transaction

A Deposit transaction is processed using an Approved Digital Acceptance Solution to credit the account of an eftpos Consumer, other than in the process for returns of goods and/or services. Unlike a Refund, a Deposit Transaction is not required to be related to a prior eftpos Transaction.

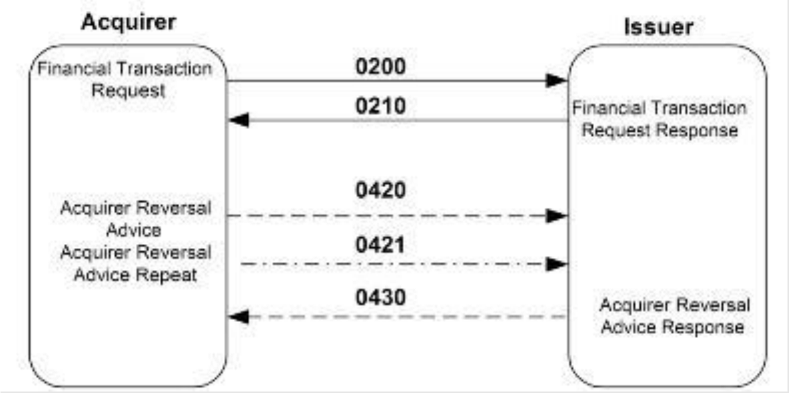

Acquirer
Issuer
Financial Transaction Request
0200
0210
Financial Transaction Request Response
0420
Acquirer Reversal Advice
Acquirer Reversal Advice Repeat
0421
0430
Acquirer Reversal Advice Response

Figure 7: Deposit Transaction flow

Deposit transactions must always be sent as Financial Transaction Requests (0200) and must not be processed as Financial Advices (0220).

6.4.9 Withdrawal Transactions

A Withdrawal transaction is processed using an Approved Digital Acceptance Solution to debit the account of an eftpos Consumer, other than in the process of performing a purchase of Cashout, Purchase, or Purchase and Cashout.

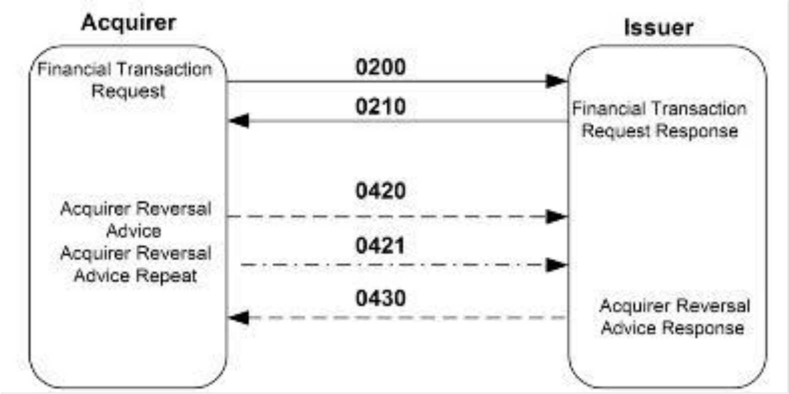

Acquirer
Issuer
Financial Transaction Request
0200
0210
Financial Transaction Request Response
Acquirer Reversal Advice
Acquirer Reversal Advice Repeat
0420
0421
0430
Acquirer Reversal Advice Response

Figure 8: Withdrawal Transaction flow

Withdrawal transactions must always be sent as Financial Transaction Requests (0200) and must not be processed as Financial Advices (0220).

6.4.10 Reconciliation Transaction

Reconciliation transactions are used between two end points of a link to notify the completion of a settlement period, and (where mutually agreed by Acquirer and Issuer) confirm the number and value of financial transactions that have been approved since the last reconciliation process occurred.

For Acquiring nodes, the reconciliation totals must not be updated until the financial transaction response message is received from the Issuing node with an approval action code.

Separate reconciliation totals and processing is required for each interface between nodes.

A sending node must maintain a set of reconciliation totals for each reconciliation date that the node is currently using in messages being sent. Similarly, the receiving node must maintain reconciliation totals for each date that it is receiving.

Each node must support reconciliation dates of the current date, plus the following day. Transactions with reconciliation dates that do not match one of these two dates may be rejected by the receiving system.

In the case of bi-lateral links (both acquiring and issuing) separate reconciliation totals must be maintained for messages sent and for those received i.e., they must not be netted.

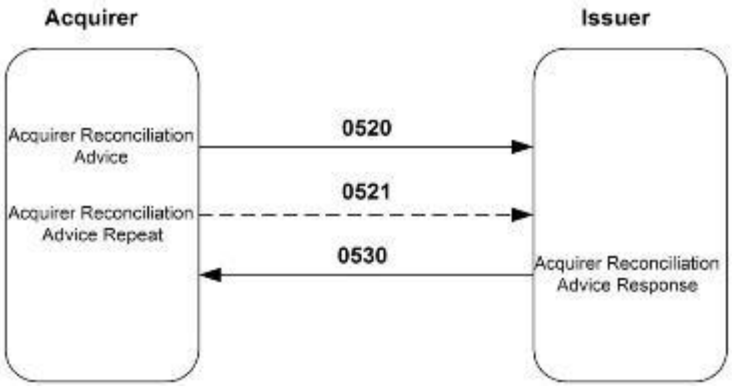

Acquirer
Issuer
Acquirer Reconciliation Advice
0520
0521
Acquirer Reconciliation Advice Repeat
0530
Acquirer Reconciliation Advice Response

Figure 9: Reconciliation Transaction flow

6.4.11 Declined ICC Transaction

For ICC originated transactions a declined transaction is any transaction where the Issuer sends, or where an ICC responds with, a response within the permitted response time, declining the transaction for reasons which may include but are not limited to, PIN errors, account errors and insufficient funds.

Where the transaction is declined by the ICC (AAC returned), the declined transaction is not to be forwarded to the Issuer, except where the merchant chooses to override the card decision in which case the fallback indicator “FBKO\” must be included in the 0220 Advice message sent to this Issuer indicating that the override has occurred. This process is known as Chip Decision Override or Fallback Override which is not permitted unless mutually agreed between the Issuer and Acquirer.

6.5. Network Management

Network Management involves the initial and ensuing dialog between the applications running at both end of the Interchange Link, which are required to start and maintain the reliable and secure flow of financial messages. It includes messages to establish and restore communications at the application layer (session establishment), the exchange of security keys, verification of link status and session termination by either node.

Network Management transactions include link Sign On/Off, Key Change Requests as well as link status (echo) requests.

A Sign On request must precede any other message type on a link and must be immediately followed with a Key Change Advice.

The eftpos Hub Link Specification details the requirements and process for network management for eftpos Hub Direct Connections.

The eftpos Secure Specifications details the requirements and process for network management for eftpos Secure Directory Server Direct Connections.

6.5.1 Sign on Request

A Sign On Request is used by a node to request permission from the receiving node to transmit financial messages. A Sign On is unidirectional and each endpoint is required to Sign On independently.

A Sign On Request performs proof-of-endpoint processing as described in Section 6.6.4.

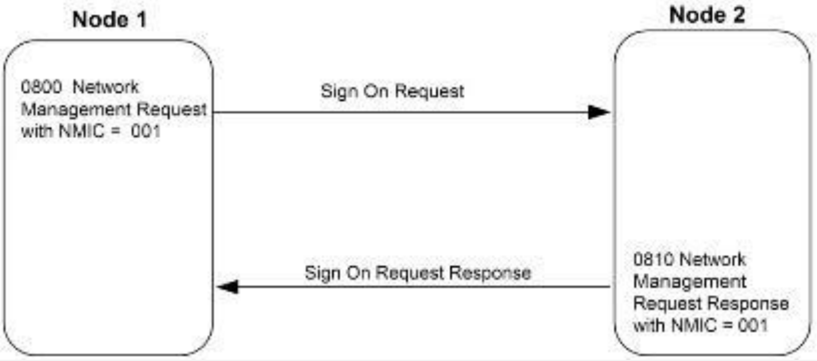

Node 1
0800 Network Management Request with NMIC = 001
Sign On Request
Node 2
Sign On Request Response
0810 Network Management Request Response with NMIC = 001

Figure 10: Sign On Request flow

A Sign On Request must precede any other message type on a link and, if successful, be immediately followed by a Key Change Request.

6.5.2 Echo Test

Echo Test transactions are used by both nodes of a link to ensure that the other node is receiving messages and responding at an application's level. They do not indicate that the link is available for use. These transactions can be sent at any time once Session Keys have been established, that is subsequent to a successful Key Change transaction.

They must be sent where no activity has occurred on the link during the preceding sixty seconds and the link is in the signed on state.

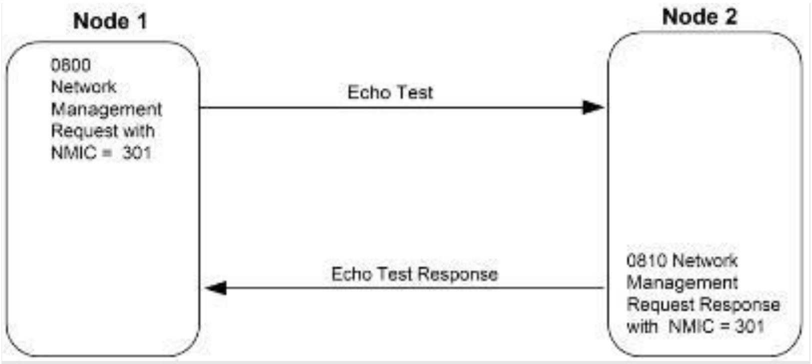

Node 1
Node 2
0800 Network Management Request with NMIC = 301
Echo Test
Echo Test Response
0810 Network Management Request Response with NMIC = 301

Figure 11: Echo Test flow

6.5.3 Key Change advice

A Key Change Advice is required after each successful Sign On, and subsequently as per intervals specified in eLS appendix C, SKC L2, to establish the session keys to be used for MAC generation/verification and PIN encipherment / decipherment as described in 6.6.3.

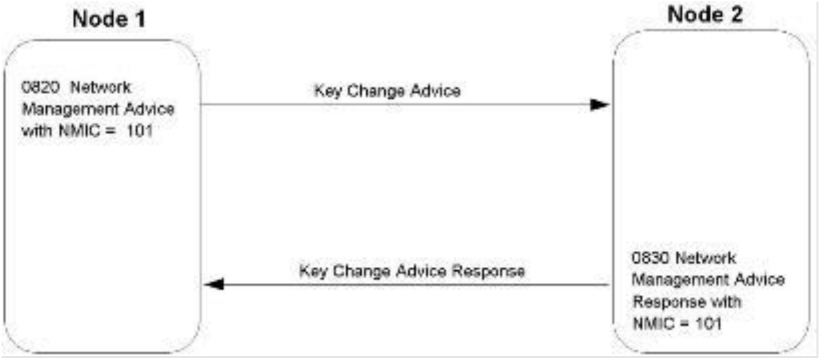

Node 1
Node 2
0820 Network Management Advice with NMIC = 101
Key Change Advice
Key Change Advice Response
0830 Network Management Advice Response with NMIC = 101

Figure 12: Key Change advice flow

6.5.4 Sign Off advice

A Sign Off advice is used by either node to terminate the transmission of financial messages in both directions.

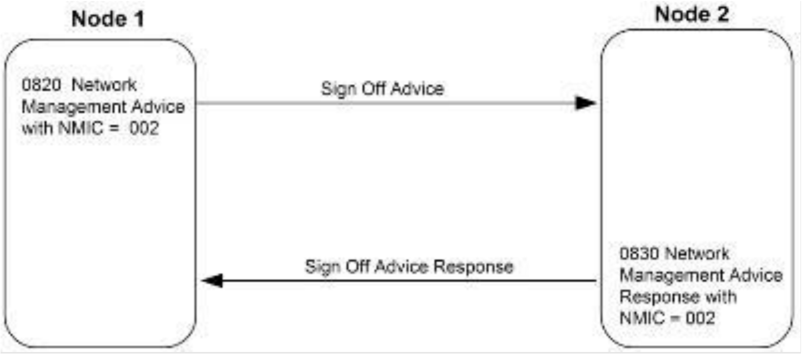

Node 1
Node 2
0820 Network Management Advice with NMIC = 002
Sign Off Advice
Sign Off Advice Response
0830 Network Management Advice Response with NMIC = 002

Figure 13: Sign Off advice

6.6. Key Management

This section describes the Interchange key management and exchange process using DEA 3 (128-bit) KEKs (Key Enciphering Keys) with proof of end-point capability. Reference can be made to AS 2805.6.3 or AS2805.6.6.

This section applies to eftpos Hub Direct Connections.

6.6.1 AS 2805 conformance

Key Management will conform to AS 2805 Part 6.1.

6.6.2 Interchange Key Encrypting Keys

Each interchange node will contain an Interchange Send Key Encrypting Key (KEKs) and an Interchange Receive Key Encrypting Key (KEKr). The Interchange Send KEK will be the same key as the Interchange Receive KEK in the partnering node, similarly the Interchange Receive KEK will be the same as the Interchange Send KEK in the partnering node. The manner by which these keys are generated and installed must be agreed between the partners and employ one of the methods identified in the eftpos Hub Link Specification

The Interchange Key Encrypting Keys are used to encipher and decipher the session keys when they are transmitted between the nodes and in the proof of end points process.

Interchange Key Encrypting Keys shall be Statistically Unique and shall be changed, at a minimum, once every two years.

Node A		Node B
Interchange Key Encrypting Key, send (KEKs)	=	Interchange Key Encrypting Key, receive (KEKr)
Interchange Key Encrypting Key, receive (KEKr)	=	Interchange Key Encrypting Key, send (KEKs)

Table 5: Interchange Key Encrypting Keys

6.6.3 Session Keys

Each node keeps four sets of Session Keys, two send sets and two receive sets.

Each set of Session Keys consists of three keys, MAC Key, PIN Protect Key and optionally a Data Enciphering Key. Each Session Key is 128-bits long and stored in a secure manner.

The send Session Key sets are generated by the sending node and numbered "1" or "2". The send Session Key sets are then forwarded to the receiving node to be used as the receive Session Key sets.

The receive Session Key sets are received in a 0820 Network Management Advice message with bit 070 equal to 101 from the sending node. The set number of either "1" or "2" contained in bit 53 indicates the receive Session Key set used by the receiving node to verify the MAC, decipher the data and translate or verify the PIN.

One set of send Session Keys is used at a time and all transactions sent from the sending node will generate the MAC and encipher the PIN, if present, using the MAC Generator Key and PIN Protect Key, respectively, from the same send Session Key set. The send Session Key set used is indicated by bit 53 (contains "1" or "2") in each message.

Session Keys must be Statistically Unique and replaced at intervals specified in eLS appendix C, SKC L2.

The Data Encipherment Key is unused. The Data Encipherment Key may optionally be included in the Key Change Message (see Network Management Key Change Advice message format 3F1.17 and 3F1.19).

When enciphered for transmission, each Session Key type will use a unique variant of the Key Enciphering Key in accordance with AS 2805 Part 6.1.

Node A	Node B
Send Session Keys Set 1	**Receive Session Keys Set 1**
MAC Key (KMACs1)	= MAC Verification Key (KMACr1)
PIN Protect key (KPEs1)	= PIN Protect key (KPEr1)
Data Encipherment Key (KDs1)	= Data Decipherment Key (KDr1)
Send Session Keys Set 2	**Receive Session Keys Set 2**
MAC Key (KMACs2)	= MAC Verification Key (KMACr2)
PIN Protect key (KPEs2)	= PIN Protect key (KPEr2)
Data Encipherment Key (KDs2)	= Data Decipherment Key (KDr2)
Receive Session Keys Set 1	**Send Session Keys Set 1**
MAC Verification Key (KMACr1)	= MAC Key (KMACs1)
PIN Protect key (KPEr1)	= PIN Protect key (KPEs1)
Data Decipherment Key (KDr1)	= Data Encipherment Key (KDs1)
Receive Session Keys Set 2	**Send Session Keys Set 2**
MAC Verification Key (KMACr2)	= MAC Key (KMACs2)
PIN Protect key (KPEr2)	= PIN Protect key (KPEs2)
Data Decipherment Key (KDr2)	= Data Encipherment Key (KDs2)

Table 6: Session Keys

6.6.4 Establishing a link

A link shall be established using the 0800/0810 Network Management Messages with a NMIC of Sign On (001). Each side must be successfully Signed On before a session can be established.

A proof of endpoints check is part of the sign on process.

A Random Number (RNs) is generated along with its inverted form (RNr) both are enciphered under KEKs. The enciphered RNs are forwarded to the interchange partner in Data Element 48 of the logon request. The enciphered RNr is stored awaiting the logon response.

The interchange partner will, on receipt of the sign on request, generate the inverted form of the enciphered RNs received (RNr) and return it, enciphered by KEKr, in the sign on response. The enciphered RNr shall be forwarded in Data Element 48.

On receiving the Sign On response, the enciphered RNr in the message is compared with the stored version of enciphered RNr. If the two values match, proof of endpoints is established.

Following these messages, the key change messages establish the current session keys. Then, and only then, can other transactions be processed.

Following is an example of the message flow to establish a link showing the key set used. The terms "send" and "receive" are from Node A's viewpoint.

Node A		Node B
0800 (Sign On)	⇒	
	⇐	0810 (Sign On Reply)
	⇐	0800 (Sign On)
0810 (Sign On Reply)	⇒	
0820 (Key Change, Send Set 1)	⇒	
	⇐	0830 (Key Change Reply)
	⇐	0820 (Key Change, Receive Set 1)
0830 (Key Change Reply)	⇒	

Node A		Node B
	⇐	0200 (Receive set 1 keys)
0210 (Send set 1 keys)	⇒	
etc.		etc.

Table 7: Establishing a link

6.6.5 Changing Session Keys

The method of Session Key changes is detailed below.

While one set of send Session Keys is being used, the other send Session Key set is randomly generated by the sending node and their KVCs generated, the keys are then enciphered under the Interchange Send KEK and transmitted to the receiving node in a 0820 Network Management Advice message.

When an 0820 message is received by the receiving node, the Session Keys are deciphered using the Interchange Receive KEK. These deciphered keys are set up as the set of receive keys specified by the set number contained in bit 53 of the 0820 message. The Key Verification Codes (KVCs) are calculated by the receiving node and transmitted to the sending node in bit 48 of the 0830 message.

When the 0830 Network Management Advice response message is received at the node initiating the key change, the KVCs contained in the 0830 message are validated. If the KVCs are correct, the new send session key set can be used immediately. If the KVCs are invalid, new send session key set must be generated and the whole process is repeated.

6.6.6 Sign Off

Either node may terminate the transmission of financial messages by sending a Sign Off Advice. A Sign Off is accomplished by the transmission of a Network Management Advice Message with a Network Management Information Code equal to 002.

6.6.7 Key Change during normal processing

A Session Key change can occur at any time; each node independently initiates the change of their send keys. The sender will advise their sending Session Keys to the receiver using a 0820 Network

Management Advice message with a NMIC for key change (101). Once a valid response (0830 message) is received and the KVCs confirmed, the new keys can be used.

6.7. Link reconciliation

Link reconciliation will be effected by the receipt of a Reconciliation Advice Message initiated by a link end-point, typically the Acquirer, once in every 24-hour period. This message contains the sender's totals (counts and the value if appropriate) of Financial and other transactions that have occurred on the link since the previous Link Reconciliation.

The Receiving party, typically the Issuer, acknowledges the Advice by sending a “0530” Reconciliation Advice Response message that contains its own totals of the transactions that it has received in the settlement period.

The eftpos Hub Link Specification details the process for Direct Connections to the eftpos Hub.

6.7.1 Link reconciliation requirements

Link Reconciliation shall comply with the following:

a. Only 0520/0521 reconciliation advice messages and 0530 reconciliation response messages shall be used in the reconciliation process.

b. Only one reconciliation advice message per logical interchange shall be sent by the Acquirer or intermediate network node, every calendar day.

c. The reconciliation advice message shall contain all the totals for that link; i.e., there is no distinction between ATM and eftpos transactions.

d. The transmission of the reconciliation advice message shall indicate the end of the reconciliation period for that Acquirer or intermediate network facility.

e. The reconciliation messages shall not be used as the sole basis of financial settlement.

f. Field 15, Date Settlement usage shall be as follows;

   i. the Acquirer, or intermediate network facility, is responsible for setting this field for all transactions being forwarded and may change the value of the field in order to forward a transaction. All transactions (requests and advices) shall contain a Date Settlement field value greater than that contained in previous reconciliation advice messages across that link. The Acquirer or intermediate network facility, may start sending financial messages with the following day's Date Settlement before closing the current reconciliation period.

   ii. the institution receiving a message may reject a transaction if the Date Settlement field contains a date prior to the current reconciliation date.

iii. all repeat transactions shall contain the same Transaction Settlement Date as their original (unrepeated) transactions.

iv. the reconciliation advice messages may be placed in a store and forward file with the aim of sending all previous advice messages with the appropriate date prior to sending the reconciliation message.

v. to ensure that all transactions are completed prior to sending the reconciliation advice message, the reconciliation advice message should not be formatted nor sent for at least the time of the timeout period and preferably for at least two minutes, after the link Transaction Settlement Date has changed for a link (cutover).

vi. where two related transactions (e.g., an original request and its reversal or a Pre-Authorised transaction and its completion advice) are transmitted either side of cutover time, the two transactions shall contain different dates in their Date, settlement fields.

g. Advice messages should be added to the settlement totals only once, when they are first sent.

h. Reversal messages should be added to the settlement totals only when the original transaction has also been added.

6.8. Link settlement times

Link Reconciliation, for the day of reconciliation shall be effected on or by 22:00 hours, or other such time as may be mutually agreed.

The eftpos Hub Link Specification details the process for Direct Connections to the eftpos Hub.

6.9. Message formats

The eftpos Hub Link Specification details the process and message formats for Direct Connections to the eftpos Hub.

7. Disputes and Chargebacks

All Issuers and Acquirers must adhere to the Disputed Transactions and Chargebacks processes and timeframes set out in the eftpos Disputed Transactions and Chargebacks Service Operations Guide.

The eftpos Disputed Transactions and Chargebacks Service Operations Guide defines the reason codes, use cases and sets out the liability allocation as between Issuers and Acquirers for Chargebacks, subject to the eftpos Issuers and eftpos Acquirer's rights and the evidentiary requirements set out in the eftpos Disputed Transactions and Chargebacks Service Operations Guide.

7.1. Issuer obligations

The Issuer must resolve a Disputed Transaction with the Acquirer using the eftpos Disputes and Chargebacks workflow tool (**eD+C**), following the processes and timeframes in the eftpos Disputed Transactions and Chargebacks Service Operations Guide. The Issuer must provide all supporting documentation required by eftpos in the applicable phase of the dispute process. Required evidence, if not provided during the dispute process, may not be eligible for consideration by eftpos should the case proceed to Arbitration.

Issuers may implement additional internal policy principles to determine whether they raise a Disputed Transaction under these Technical, Operational and Security Rules.

The Issuer must, when attempting to resolve a Disputed Transaction and, as far as practicable, avoid referral directly back to the Merchant, provided that the eftpos Consumer has already raised and attempted to resolve complaints about goods or services not received and goods or services not as described directly with the Merchant.

The Issuer must:

a. establish where the value for the Disputed Transaction is held e.g. establish that the value is not held as a result of an internal or settlement error;

b. upon decision to raise a case within eD+C, enter the data elements as detailed in the eftpos Disputed Transactions and Chargebacks Service Operations Guide to search for and identify the Transaction to dispute:

c. attach evidence as required by the eftpos Disputed Transactions and Chargebacks Service Operations Guide, excluding any Personal Information, and submit the case to the eftpos Acquirer in eD+C; and

d. respond to the Acquirer within the required timeframes in clause 7.4. The case will automatically be closed in favour of the Acquirer if the eftpos Issuer does not respond within these timeframes.

7.1.1 Permitted Chargebacks

An eftpos Transaction shall be disputed by an Issuer, using one of the reasons listed below. Details of the Reason Codes, applicable use cases, and the evidence required to support or challenge a Disputed Transaction are set out in the eftpos Disputes and Chargebacks Service Operations Guide.

7.1.1.1 Consumer raised disputes

An Issuer may dispute a Form Factor present or Card Not Present eftpos Transaction on behalf of an eftpos Consumer for the reasons listed below:

Form Factor Present

a. Consumer does not recognise the Merchant;

b. Duplicate Transaction;

c. Paid by other means;

d. Non-dispense or partial dispense of cash (Merchant self-service device only);

e. Non-delivery or partial delivery of goods/service;

f. Goods/service not as described, including Merchant no longer trading/absconded/insolvent;

g. Transaction amount on eftpos Consumer's statement differs from transaction receipt;

h. Refund not received;

i. Deposit Short pay;

j. Transactions not compliant with eftpos Rules.

Card Not Present

a. Fraud;

b. Consumer does not recognise the Merchant;

c. Duplicate Transaction;

d. Transaction amount on Consumer statement differs from their receipt;

e. Unauthorised Transaction;

f. Refund not received;

g. Non-delivery or partial delivery of goods/service;

h. Cancelled Payment Arrangement;

i. Deposit Short pay;

j. Goods/service not as described, including Merchant no longer trading/absconded/insolvent; and

k. Transactions not compliant with eftpos Rules.

7.1.1.2 Issuer raised disputes

Where a Fallback Transaction that is not compliant with these Technical, Operational and Security Rules has been performed an Issuer may dispute the Transaction. The eftpos Consumer's account must have become overdrawn as a direct result of this Transaction, and the Issuer must have attempted to recover the funds from the eftpos Consumer before raising a dispute relating to an invalid Fallback Transaction. The reasons for which an Issuer may dispute a Fallback Transaction are listed below:

a. Split transactions;

b. Unauthorised Transaction; and

c. Incomplete Short Duration Pre-Authorised Transaction (Purchase/Reversal/Advice).

d. Transactions not compliant with eftpos Rules.

e. Where a Deposit transaction has been performed and the Issuer determines that the funds cannot be retained due to application of Law, the Issuer may raise a Disputed Transaction and must return the funds using the Chargeback mechanism to the Acquirer within timeframes required by Law and in any event within five Business Days of the Transaction date.

7.1.2 Instances where a Chargeback is not permitted

The Issuer is not permitted to Chargeback transactions where:

a. the Issuer has provided an approved authorisation response to the Acquirer under Section 2.12.6.2 (unless the Transaction was subsequently declined by the card's Chip in the case of eftpos Chip and Contactless cards);

b. the Cardholder raises a Disputed Transaction more than 210 days after date of the eftpos Transaction giving rise to the dispute;

c. there are insufficient details to identify the Disputed Transaction;

d. the Issuer has performed Strong Customer Authentication or Transaction Authentication at the time of the Transaction, in respect of an eftpos Digital Transaction disputed as Fraud. For clarity, where Cardholder Authentication was performed previously on the first transaction of Payment Arrangement, a Chargeback may still be permitted on any subsequent transaction in the Payment Arrangement unless Cardholder Authentication was performed on the subsequent transaction;

e. for Multi-Network Debit Cards, from 01 November 2021, the Issuer has performed Cardholder Authentication using eftpos Secure in respect of an eftpos Digital Transaction disputed as Fraud;

f. For Multi-Network Debit Cards, from 01 November 2021, the Merchant requested the Issuer to perform Cardholder Authentication using eftpos Secure in respect of an eftpos Digital Transaction disputed as Fraud;

g. For eftpos Proprietary Cards, from 01 May 2022, the Issuer has performed Cardholder Authentication using eftpos Secure in respect of an eftpos Digital Transaction disputed as Fraud; or

h. For eftpos Proprietary Cards, from 01 May 2022, the Merchant requested the Issuer to perform Cardholder Authentication in respect of an eftpos Digital Transaction disputed as Fraud.

i. The Issuer cannot dispute an eQR transactions for fraud where the transaction is considered an eQR authenticated transaction (Refer to clause 3.10.7)

7.2. Acquirer obligations

The Acquirer must:

a. promptly initiate investigations when a case is received from an eftpos Issuer through eD+C.

b. liaise with the Merchant if required to obtain additional information to the Disputed Transaction. If additional information is required from the Merchant, 10 days will be added to the case timer, to support the additional investigations. Where a case has not been actioned by the eftpos Acquirer within the timeframes at clause 7.4, the case will be automatically closed in favour of the Issuer and a Chargeback raised; and

c. Provide evidence as set out in the eftpos Disputed Transactions and Chargebacks Operations Guide applicable to the Reason Code for the dispute, in the response to the eftpos Issuer via eD+C. The eftpos Acquirer must provide all supporting documentation required by the Company in the applicable phase of the dispute process. Required evidence, if not provided during the dispute process, may not be eligible for consideration by the Company should the case proceed to Arbitration.

7.2.1 Re-presentment rights

From the effective date of eD+C, Acquirers will no longer need to process re-presentments relating to eftpos Disputed Transactions and Chargebacks, due to the following:

a. For eftpos Form Factor present and eftpos Card-Not-Present cases, the funds remain with the eftpos Acquirer unless and until the case is closed in favour of the eftpos Issuer; and

b. For eftpos Card-Not-Present cases arising from fraud, and in advance of Strong Customer Authentication implementation where the Issuer has had an opportunity to perform Cardholder Authentication at the time of transaction, the Acquirer can retain the right to:

   i. Not challenge the eftpos Card-Not-Present fraud Disputed Transaction and accept liability if there is no case to argue.

   ii. Not challenge the eftpos Card-Not-Present fraud Disputed Transaction and accept liability if the Acquirer evidence does not meet the evidence list defined in the eftpos Disputes and Chargebacks Operations Guide.

   iii. Challenge the eftpos Card-Not-Present fraud Disputed Transaction if there is adequate compelling evidence as described in the eftpos Disputes and Chargebacks Operations Guide that supports that the Cardholder claim is invalid.

7.3. Pre Arbitration and Arbitration

An Issuer may initiate Pre-Arbitration as per the below:

a. if the dispute has followed all steps in the workflow (i.e. it has been reviewed and challenged by the Issuer and Acquirer twice) within the specified timeframe and has not been resolved.

If there is no resolution achieved from Pre-Arbitration the case shall proceed to Arbitration and the action shall be performed by eftpos. The procedure and timeframe to close the Pre-Arbitration and Arbitration should be followed as described in the eftpos Disputes and Chargebacks Operations Guide.

All Arbitration cases must be processed through eD+C.

7.4. Timing

Timing of processing Disputed Transactions is governed by these Technical, Operational and Security Rules which reflect the ePayments Code.

The eD+C workflow tool will facilitate timely resolution of Disputed Transactions and Chargebacks in accordance with the eftpos Disputed Transactions and Chargebacks Service Operations Guide. The timelines for resolution of cases through eD+C are set out below and reflect the ePayments Code. For the purposes of disputed eftpos Transactions a day means a calendar day.

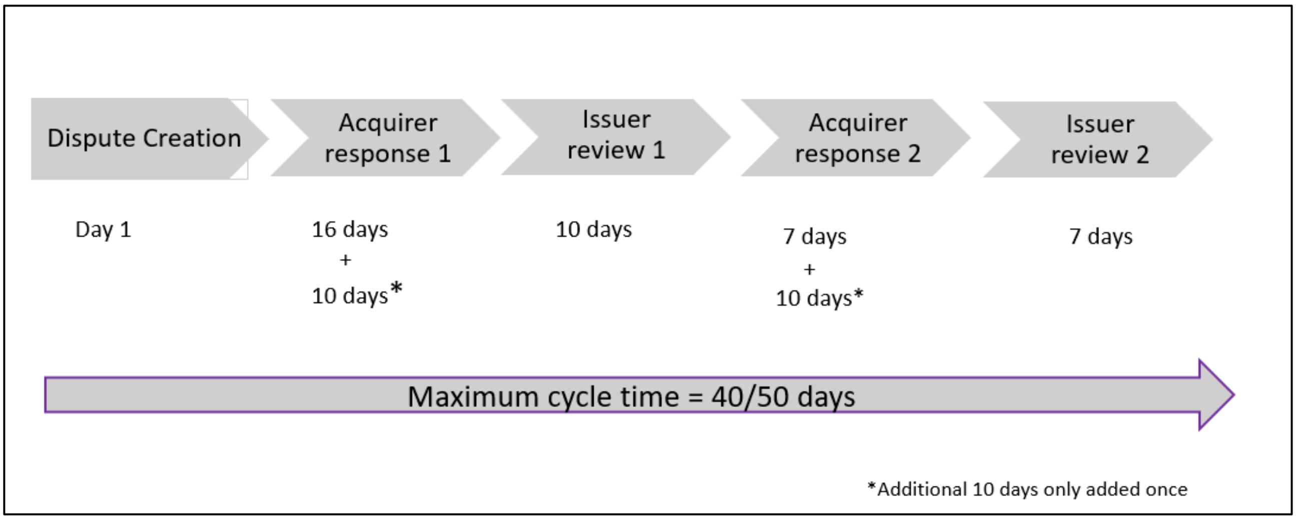


Figure 14: eftpos Disputed transactions maximum timeframes

7.5. On-Us Disputed Transaction processing

Members must process On-Us disputes entirely within their own internal systems.

7.6. Retention of records

Unless a longer retention period is required by applicable legislation or the Member's own policies, Fallback vouchers, forms and reports as well as Disputed Transaction information are to be retained in a suitable format for at least 12 months.

7.7. Privacy compliance

In addition to clause 2.7, Members using the eD+C tool, represent and warrant that they have authority from the relevant individual to collect and disclose to the Company any Personal Information input into the eD+C tool for the purposes of resolution of Disputed Transactions and Chargebacks and for the Company to use the information in an aggregate form for data analytics for the purposes of the eftpos Payment System and for product or service improvement or delivery.

7.8. Chargebacks monitoring program

The eftpos Chargebacks monitoring programs defines acceptable tolerances for Chargebacks volumes under which Acquirers must operate.

Each quarter (calendar quarter) the Company will make available to each Acquirer Member, a quarterly Chargebacks reporting dashboard and portfolio quality report which outlines their performance to the program. Acquirers who breach these programs will be required to provide to the Company a Member action plan at both the warning threshold and breach threshold, outlining actions being taken to bring Chargebacks below thresholds. Acquirers are required to submit action plans within one (1) calendar month of receiving the breach notification from the Company.

These action plans shall be submitted via email to: fraud@eftposaustralia.com.au

The program is set out below, and further requirements and documentation are referenced within the eftpos Disputed Transactions and Chargebacks Service Operations Guide.

Any Merchant	Warning threshold	Breach threshold
Chargeback rate (Transactions)	**75** bps (+>75cbks)	**150** bps (+>1000cbks)
Breach period consecutive quarters	2	3
Measurement method	Member Portfolio Quality Reports and Performance Dashboards	Member Portfolio Quality Reports and Performance Dashboards
Member Requirement	Completion of Member Action Plan Template when in breach of warning threshold	Completion of Member Action Plan Template when in breach of warning threshold
Consequence		Breach notification and fine decision as set out in the Scheme Rules – Part D Clause 16 Fines.

8. Settlement

8.1. General principles

8.1.1 Settlement each RITS business day

Settlement for eftpos Transactions will be performed on each RITS Business Day in accordance with the eftpos Scheme Rules and this Part 8 of these Technical, Operational and Security Rules.

8.1.2 Timing of settlement of eftpos Transactions

a. Settlement of the eftpos Batch will occur on the first RITS Business Day after the Batch Recorded Date attributed to the eftpos Transaction. Clearing Interest is calculated for the number of days between the Batch Recorded Date and the date of Settlement of the eftpos Batch and is added to the net Settlement obligation. See Table 8.

b. Settlement of eftpos Transactions that Members settle bilaterally after an Insolvency Event, inclusive of Clearing Interest, is due on or before the first RITS Business Day after the date specified in the eftpos Transaction message as the Transaction Settlement Date, unless otherwise notified by the Company after deferral of Settlement.

c. As between Settlement Agents and their represented Indirect Settlers:

    i. Payment to Indirect Settlers of amounts received in Settlement by the Settlement Agents on behalf of Indirect Settlers is due at a time negotiated between the Settlement Agent and Indirect Settler, inclusive of Clearing Interest and adjusted for any fees or amounts due in Settlement between the Settlement Agent and the Indirect Settler; and

    ii. Payment to Settlement Agents of amounts to be paid in Settlement on behalf of Indirect Settlers, inclusive of Clearing Interest, and any fees or other amounts payable between the Settlement Agent and the Indirect Settler are a matter for negotiation between the Settlement Agent and their Indirect Settlers.

8.2. Direct Settlers appointed to settle on behalf of Members – Settlement Agents

For the avoidance of doubt, the arrangements between a Direct Settler (the Settlement Agent) and a Member (the Indirect Settler) that has appointed the Settlement Agent to settle on its behalf are to be agreed between the Indirect Settler and the Settlement Agent, provided that they are consistent with these Technical, Operational and Security Rules. In each and every case any such Settlement Agent:

a. must be a participant that has direct contractual relationship with eftpos; and

b. assumes the liabilities and Settlement obligations of each of its Indirect Settlers in respect of eftpos Batch Settlement as if it were the Indirect Settler.

8.3. Agreed Settlement Cut-over Times

8.3.1 No longer used

8.3.2 Settlement of eftpos transactions processed using the eftpos Hub

The Settlement Cut-over Time for eftpos Transactions processed through the eftpos Hub is determined by each Acquirer and agreed with the Company as part of the Standard Direct Connections Project, but must be prior to 21:50 each calendar day. The process to effect Settlement Cut-over is set out in the eftpos Hub Link Specification.

8.4. Settlement and Interchange reports

8.4.1 Bilateral Interchange Links

Each Member that is a Direct Settler under a Bilateral Agreement for Settlement must produce:

a. an Interchange Settlement Report for each RITS Business Day which details the total number of eftpos Transactions and total value of eftpos Transactions for the purposes of Interchange Fee calculation; and

b. a Bilateral Settlement Report, (netted for credits and debits) with each bilateral counterparty, for eftpos Transactions processed through its Interchanges (or the Interchanges used by a Member that has appointed it to settle on its behalf), as at the agreed Settlement Cut-over Time for each Interchange.

8.4.2 Direct Connections to the eftpos Hub

The Company will use the eftpos Transaction data captured by the eftpos Hub to produce and provide to each eftpos Issuer and eftpos Acquirer:

a. each calendar day the reports referred to in the eftpos Hub Files and Reports – POS Specification, including:

   i. a daily Interchange Settlement Report (SR100) containing the following information for the relevant Member:

      A. the total value of each eftpos Transaction type acquired by that eftpos Acquirer attributed to that Settlement Date with each eftpos Issuer; and

      B. the total value of each eftpos Transaction type performed by customers of that eftpos Issuer attributed to that Settlement Date with each eftpos Acquirer;

b. before 3a.m. each RITS Business Day, a Batch Participant Report (BR100-01 for a Primary Batch or BR101-01 for a Secondary Batch) for each eftpos Batch Participant containing for the relevant eftpos Batch Participant and all Indirect Settlers and Non-clearers represented by that eftpos Batch Participant:

   i. the total amount to be exchanged in Settlement for each calendar day since the last RITS Business Day with each other eftpos Batch Participant;

   ii. any Clearing Interest with each other eftpos Batch Participant, in accordance with Table 8;

   iii. total Clearing Interest for that eftpos Batch Participant; and

   iv. the net value to be paid or received by that eftpos Batch Participant for the eftpos Batch Settlement for that RITS Business Day;

c. before 3a.m. each RITS Business Day, a Batch Agency Report (BR100-02 for a Primary Batch or BR101-02 for a Secondary Batch) for each Direct Settler and Indirect Settler pairing containing:

   i. the total amount to be exchanged in Settlement for each calendar day since the last RITS Business Day by the Direct Settler on behalf of the Indirect Settler;

   ii. any Clearing Interest between the Direct Settler on behalf of the Indirect Settler with each other eftpos Batch Participant, in accordance with Table 8;

iii. total Clearing Interest for that Indirect Settler; and

iv. the net value to be paid or received by the Direct Settler on behalf of that Indirect Settler for that RITS Business Day; and

d. each RITS Business Day, an Interchange Fee Report for each Member, in reliance on which Members must pay Interchange Fees;

e. each week on the first RITS Business Day after Tuesday, a Scheme Fee report for each Tier 1 Member which must pay the Scheme Fees (including ATM processing fee) arising from eftpos Transactions during the preceding week (i.e. from Tuesday to Monday) to the Company.

f. The weekly scheme fees report on or after the first Tuesday of each month will include any other Fees owed to the Company at that time, including but not limited to the Infrastructure fee;

g. a monthly report on the 3rd calendar day of each month consisting of scheme fees, infrastructure fees, ATM processing fee and Dispute & Arbitration fee for the previous month; and

h. a monthly report on the 3rd calendar day of each month consisting of the interchange fees paid or received by the Member during the previous month.

For report format and detail, Members should refer to the eftpos Hub Files and Reports – POS Specification

8.5. Net settlement

8.5.1 Net settlement under bilateral agreements

Settlement of eftpos Transactions processed through a bilateral Interchange Link (rather than Direct Connections to the eftpos Hub) must be inclusive of Clearing Interest. Such Settlement must be on a net basis for all credits and debits between the relevant counterparties to the eftpos Transactions.

8.5.2 Net settlement using the eftpos Batch in RITS

Prior to 07:30 on each RITS Business Day, the Company will create a RITS Instruction providing the net position of each eftpos Batch Participant calculated using the Batch Participant Reports referred to in clause 8.4.2. An example of the typical RITS Instruction schedule for an ordinary week is set out below:

a. Where an eftpos Batch Participant wishes to raise a dispute about the value of its Settlement obligation, clause 8.8 will apply.

b. The eftpos Batch Settlement will only occur if the Company has submitted the RITS Instruction to RITS and all net payers have sufficient funds in their ESA to settle. Settlement of the eftpos Batch can occur at any time between 7:30am and 4:30pm (excluding the period between 8:45am and 9:15am) on a RITS Business Day.

c. If an eftpos Batch Participant does not have sufficient funds in their ESA to fulfil their Settlement obligations (and those of Indirect Settlers and Non-clearers that the eftpos Batch Participant represents), by 12 noon on a relevant RITS Business Day, the Company will consider whether an FTS Event has occurred in respect of that eftpos Batch Participant and, if the Company notifies Members that an FTS Event has occurred, clause 8.11 will apply.

RITS Instruction submitted prior to start of day	Days being settled	Days Clearing Interest Applied
Monday	Friday	3
Tuesday	Saturday, Sunday, Monday	1
Wednesday	Tuesday	1
Thursday	Wednesday	1
Friday	Thursday	1

Table 8: Net settlement using the eftpos Batch in RITS

8.6. Settlement procedures

8.6.1 eftpos Settlement Service

8.6.1.1 RITS instruction submitted to RITS Batch feeder

a. This clause applies from the RITS Business Day that the eftpos Settlement Service becomes operational.

b. The Company will aim to submit to RITS the RITS Instruction prior to 7:30am on each RITS Business Day.

c. RITS will validate the RITS Instruction and place it on the RITS system queue and activate the eftpos Batch Settlement at 7:40am.

d. Each eftpos Batch Participant will be able to view its final multilateral net position against the eftpos Payment System (for itself and each Indirect Settler or Non-clearers on whose behalf it settles) for the eftpos Batch (inclusive of Clearing Interest) in RITS from the time of activation of the eftpos Batch Settlement (expected to be 7:40am, provided the eftpos Batch Settlement RITS Instruction has not been rejected and not yet re-submitted).

e. RITS will test availability of funds in each eftpos Batch Participant's ESA for Settlement throughout the day, except during the time reserved for the 9:00am Settlement.

f. If the Company is unable to submit a RITS Instruction to the RITS Batch Feeder prior to RITS opening on that RITS Business Day, the Company will notify all Batch Participants and the RBA and nominate a date and time by which the Company will submit the RITS Instruction. eftpos Batch Participants agree that the RITS Instruction may be submitted later on the same RITS Business Day or carried over to the next RITS Business Day.

8.6.1.2 Rejection of RITS Instructions

If a RITS Instruction is rejected by the RITS Batch Feeder, the Company will promptly:

a. notify all eftpos Batch Participants of the rejection, together with an estimate of the date and time for a revised RITS Instruction to be submitted;

b. review and rectify any defects in the original RITS Instruction;

c. submit a revised RITS Instruction; and

d. notify all eftpos Batch Participants when the revised RITS Instruction has been submitted.

8.6.1.3 Recalling and replacing a RITS Instruction

a. Subject to the rules governing RITS, the Company may recall any RITS Instruction using a RITS Recall Instruction prior to Settlement of that RITS Instruction.

b. Without limiting the circumstances in which the Company may recall any RITS Instruction, the Company will generally only recall any RITS Instruction in the event of:

c. an FTS Event; or

d. the Company needing to submit a revised RITS Instruction.

e. If the Company submits a RITS Recall Instruction, it will promptly notify the eftpos Batch Participants and the RBA, and advise the reason for the recall, together with an estimate of the date and time for a revised RITS Instruction to be submitted.

8.6.1.4 Member obligations

a. eftpos Batch Participants must fund their ESA to enable eftpos Batch Settlement by 8:45am each RITS Business Day and otherwise not alter the priority status communicated in the RITS Instruction if doing so would mean that the eftpos Batch Participant does not have or no longer has sufficient funds in their ESA to settle their calculated Settlement obligation for eftpos Transaction on the relevant RITS Business Day.

b. Each eftpos Batch Participant must have sufficient funds in its ESA to fulfil the Settlement obligations, of that Member and each Indirect Settler or Non-clearer on behalf of whom it settles, by 8:45am on each RITS Business Day, irrespective of any disputes or discrepancies.

c. If the Company recalls a RITS Instruction and replaces it with another RITS Instruction in accordance with these Technical, Operational and Security Rules, the Direct Settler must fund their ESA to enable eftpos Batch Settlement to occur within the same RITS Business Day.

8.6.2 Clearing interest

a. For the purpose of determining how to apply Clearing Interest, eftpos Transactions authorised on a weekend or public holiday shall be treated as if they had been authorised on the first RITS Business Day occurring after the weekend or public holiday.

b. On the first RITS Business Day after the weekend or public holiday, eftpos Transactions authorised on the last RITS Business Day prior to the weekend or public holiday shall be settled, with Clearing Interest applying to all intervening calendar days.

c. On the second RITS Business Day after the weekend or public holiday, all eftpos Transactions authorised during the weekend or public holiday, or on the first RITS Business Day after the weekend or public holiday shall be settled, with Clearing Interest applying to the number of calendar days between the first and second RITS Business Days after a weekend or public holiday, (i.e. 1 days Clearing Interest is applied, except when a public holiday occurs on a Thursday, such that the first subsequent RITS Business Day is a Friday, and the second subsequent RITS Business Day is a Monday, in which case 3 days Clearing interest is applied).

For example, eftpos Transactions authorised on the Thursday before Good Friday will be settled on the following Tuesday, with 5 days Clearing Interest applied, and eftpos Transactions occurring on Good Friday to the following Tuesday inclusive shall be settled on Wednesday with 1 days Clearing Interest applied. See Table 8.

8.7. Fallback Transactions

Settlement for Fallback Transactions exchanged manually i.e. not exchanged via Electronic Fallback processing, are to be effected using direct remittance drawing, warrant or other mutually agreed means.

Electronic Fallback Transactions are to be included in the daily Interchange Settlement Reports and settled as part of the eftpos Batch Settlement.

8.8. Reconciliation and resolution of Settlement discrepancies

8.8.1 eftpos Transactions processed through a bilateral Interchange Link

In situations where a Settlement discrepancy has occurred between Members using a bilateral Interchange Link (between a Direct Settler and either a Non-Clearer or an Indirect Settler; or between Direct Settlers following an FTS Event), the Members must exchange the details set out in Clause 8.8.3 for each eftpos Transaction logged within their system for items exchanged between them using that bilateral Interchange Link during the Settlement period to which the discrepancy relates. Any adjustment following resolution of a Settlement discrepancy must be notified to the Company and must be included in Settlement between the parties to the Settlement discrepancy on the next RITS Business Day.

8.8.2 eftpos Transactions processed through the eftpos Hub

a. For Settlement discrepancies relating to eftpos Transactions processed through the eftpos Hub, Tier 1 Members as referenced in Clause 1.8 of the eftpos Scheme Rules must:

   i. if they are an eftpos Batch Participant, fulfil their Settlement obligation contained in the RITS Instruction; or

   ii. notify the Company within two Business Days on the number published by the Company from time to time for the Company to facilitate the resolution of the discrepancy or to check the details set out in clause 8.8.3 of each eftpos Transaction logged through the eftpos Hub for the items exchanged between those Members during the Settlement period to which the discrepancy relates; and

   iii. co-operate with the Company and any counterparty to a discrepancy to resolve the discrepancy.

b. Where the discrepancy arises as a result of an error, an adjustment must be affected as follows:

   i. where the error is not an Error of Magnitude and the impacted Members agree that an error has occurred and will be adjusted, adjusting payments will be made between the impacted

Members in the manner agreed between them, without Clearing Interest. Such adjustments will be effected by:

A. whichever impacted Member identifies the error notifying the Company and each other impacted Member immediately once the details of the error are known;

B. once an error is agreed by all impacted Members and the Company, an adjustment must be effected in the manner agreed between impacted Members with notification to the Company; and

C. the impacted Member fulfilling their Settlement obligation in the eftpos Batch Settlement;

ii. where the error is an Error of Magnitude and the impacted Members agree that an error has occurred and will be adjusted, adjusting payments will be made between the impacted Members in the manner agreed between them, together with Clearing Interest. Such adjustments will be affected by:

A. whichever impacted Member identifies the error notifying the Company and each other impacted Member immediately once the details of the error are known;

B. once an error is agreed by all impacted Members and the Company, an adjustment must be agreed between all impacted Member and the Company on a multi-lateral net basis between all impacted Members;

C. the adjustment will then be effected by all impacted Members notifying their respective treasury areas of the size of the error and agreeing the date for the Settlement of the adjustment;

D. treasury areas will then settle the adjustment in ESA funds as a treasury-based ESA cash transfer in RITS;

iii. where the Company becomes aware that an error has occurred in a settled batch and the impacted Members have not invoked sub-clauses (i) or (ii) above the Company will:

A. notify eftpos Batch Participants that it is performing an adjustment via a Corrective Batch), including providing details of the impacted eftpos Batch Settlement;

B. calculate the required netted adjustment to be effected through a Corrective Batch, that will bring the eftpos Member's Settlement position to that which would have occurred have the original Settlement been correct (inclusive of Clearing Interest);

C. notify all impacted eftpos Batch Participants of the adjustment amount and the nominated RITS Business Day for settlement of the adjustment through the Corrective Batch; and either:

1. include the adjustment in the earliest possible Batch Participant Reports, Batch Agency Reports and submit to RITS the Corrective Batch, on the earliest possible RITS Business Day after the Company became aware of the error; or

2. require impacted Members to invoke the payment mechanism referred to in sub-clauses (i) or (ii) above; and

3. on receipt of notices from the Company above, each impacted eftpos Batch Participant must comply with the notices from the Company and either fund their ESA, including the adjustment as notified by the Company in the Batch Participant Reports, Batch Agency Reports and RITS Instruction or initiate the RTGS transfer to enable Corrective Batch Settlement to occur on the nominated RITS Business Day.

c. for clarity, a Corrective Batch will not be submitted if a Secondary Batch is or has been submitted. A Corrective Batch will never be split to create a Secondary Batch, even if it has not settler, for example is a Batch Participant has insufficient funds. If the Corrective Batch does not settle by the close of a RITS Business Day, a new Corrective Batch (using the same input values, with an extra days' Clearing Interest) will be calculated and submitted the next RITS Business Day.

d. Disputes relating to Disputed Transactions and Chargebacks will be resolved according to Part 7 of these Technical, Operational and Security Rules. From the date notified by the Company, once Chargebacks are resolved and the relevant Issuer or Acquirer have notified the Company of acceptance of the Chargeback, the Company will include the Chargeback in the RITS Instruction for the next RITS Business Day.

e. This provision applies without prejudice to the right of any party to invoke the dispute resolution procedures in Clause 39 of the eftpos Scheme Rules.

8.8.3 Details to be provided to reconcile Settlement discrepancies

Transaction details to be provided to enable reconciliation where discrepancies have been identified by Issuers are:

a. Cardholder number (truncated to conform with PCI DSS, unless the Issuer has requested to receive and entered an opt-in agreement with the Company to receive an encrypted AR 100 file variant including the full unmasked PAN)

b. Transaction Amount

c. Transaction Response Code

d. Terminal Identification Number (TID)

e. Transaction date and time

f. Acquirer reference number

g. Terminal sequence number (if available)

8.9. Disabling Events

Members suffering a Disabling Event must invoke their business continuity and disaster recovery plan (maintained in accordance with Clause 28.13 of the Scheme Rules and Clause 2.11 of these Technical, Operational and Security Rules) such that their ability to fulfil Settlement obligations is not impeded. Members must notify the Company if their business continuity plan is invoked. A Disabling Event may be a Potential FTS Event. Clause 8.11.2(e) applies to a Disabling Event.

8.10. References to time

For the purpose of this Section 8 a reference to any time of day is a reference to local time in Sydney.

8.11. Failure to settle and Deferral of Settlement

8.11.1 Not in use

8.11.1.1 Application of clause

This Clause 8.11 applies in connection with the occurrence of any FTS Event or Potential FTS Event. In addition, the Company has published a set of FTS Guidelines to assist Members in preparing for and dealing with the occurrence of an FTS Event or Potential FTS Event. Members should ensure that they have a continuing full understanding of the FTS Rules and the FTS Guidelines.

8.11.1.2 Member's obligations

To the extent it is legally able to do so, each Issuer Member and Acquirer Member must act in accordance with this clause 8.11 if any Member is unable to discharge its Settlement obligations arising from eftpos Transactions at the prescribed time in accordance with the eftpos Scheme Rules and these Technical, Operational and Security Rules.

8.11.2 Deferral by the Company of Settlement

a. **When can Settlement be deferred:** The Company may, but is not obliged to, defer Settlement if an FTS Event, Potential FTS Event or a Disabling Event occurs or pending resolution of whether an FTS Event has occurred. Additionally, Settlement may be deferred if Settlement does not occur before the end of a RITS Business Day.

b. **Investigation by the Company:** If the Company is notified or otherwise becomes aware of a Potential FTS Event or a Disabling Event, the Company will work to confirm whether or not an FTS Event has occurred in respect of Members impacted by a Potential FTS Event and/or work to confirm recovery following the Disabling Event in respect of Members impacted by the Disabling Event.

c. **Authority from Members:** Each Member authorises the Company to discuss with the RBA deferral in respect of all Members' Settlement obligations under the eftpos Payment System in the event of a Potential FTS Event or a Disabling Event.

d. **Timing of deferral decision:** Any decision by the Company to defer Settlement will occur before 4:30pm on the relevant RITS Business Day. If no decision is made to defer Settlement and the eftpos Batch Settlement does not occur before the end of a RITS Business Day, then clause 8.11.3 will apply.

e. **Deferral before FTS Event:** If Settlement is to be deferred for a Potential FTS Event or for a Disabling Event (before any determination of whether an FTS Event has occurred), the Company will:

   i. notify all Members and the RBA and APRA of the deferral of Settlement for all eftpos Transactions, together with an estimate of the date and time for revised Settlement, including for submission of a revised RITS Instruction;

   ii. recall any RITS Instruction submitted by the Company to RITS for the impacted RITS Business Day for a Primary Batch;

   iii. give notice to each Issuer and Acquirer that the Batch Participant Reports for each Issuer and Acquirer, the Batch Agency Reports for each Settlement Agent and any RITS Instruction submitted by the Company to RITS for the impacted RITS Business Day for a Primary Batch has been recalled;

   iv. calculate Clearing Interest for the period between the RITS Business Day from which Settlement was deferred and the RITS Business Day to which Settlement is deferred;

   v. re-calculate the Batch Participant Reports for each Issuer and Acquirer, the Batch Agency Reports for each Settlement Agent and any RITS Instruction, together with Clearing Interest for eftpos Batch Settlement to run on the next RITS Business Day after deferral of Settlement;

   vi. provide the revised Batch Participant Reports and Batch Agency Reports and submit the revised RITS Instruction for Settlement of eftpos Transactions for the deferred Settlement in accordance with the Scheme Rules and these Technical, Operational and Security Rules on the RITS Business Day to which Settlement is deferred. On that RITS Business Day, the Primary Batch will contain any carry over Settlement obligations resulting from the deferral as well as the Settlement obligations for the RITS Business Day on which the Primary Batch is submitted; and

vii. notify all eftpos Batch Participants when the RITS Instruction for the deferred eftpos Batch Settlement has been submitted.

f. **Deferral after FTS Event:** If the Company decides to defer Settlement of eftpos Transactions following the occurrence of an FTS Event in respect of one DSEP only, the Company will promptly:

i. notify all Members, the RBA and APRA of the deferral, together with an estimate of the date and time for revised Settlement, including for submission of a revised RITS Instruction; and

ii. give notice that the Batch Participant Reports for each Member, the Batch Agency Reports for each Settlement Agent and the RITS Instruction submitted by the Company to RITS for the impacted RITS Business Day (whether for a Primary Batch, Secondary Batch or DSEP Batch) will lapse;

iii. calculate Clearing Interest for the period between the RITS Business Day from which Settlement was deferred and the RITS Business Day to which Settlement is deferred;

iv. re-calculate the Batch Participant Reports for each Member, the Batch Agency Reports for each Settlement Agent and any RITS Instruction, in each instance, together with any Clearing Interest:

A. for a Primary Batch in the case of an FTS Event which is a Statutory Management, to run on the next RITS Business Day after deferral of Settlement;

B. for Secondary Batch and DSEP Batch in the case of an FTS Event other than an Insolvency Event, to run on the next RITS Business Day after deferral of Settlement; or

C. for a Primary Batch excluding the DSEP, to run on the next RITS Business Day after deferral of Settlement and a DSEP Report to be settled bilaterally at the election of the Survivors in the case of an FTS Event which is an Insolvency Event other than a Statutory Management;

v. provide the revised Batch Participant Reports and Batch Agency Reports and submit the revised RITS Instruction for Settlement of eftpos Transactions for the deferred Settlement in accordance with the Scheme Rules and these Technical, Operational and Security Rules on the RITS Business Day to which Settlement is deferred; and

vi. notify all eftpos Batch Participants when the RITS Instruction for the deferred eftpos Batch Settlement has been submitted.

8.11.3 Procedural failed Settlement

If an eftpos Batch Settlement (of any type) is not deferred under Clause 8.11.2 and is not otherwise settled in accordance with this Section 8 prior to the closure of RITS on the RITS Business Day that the RITS Instruction is submitted, the RITS Instruction for that batch will be automatically removed from RITS.

In this case, all Settlement obligations in the batch which did not settle must be resubmitted on the next RITS Business Day, together with Clearing Interest applied for each calendar day that the batch was delayed. This means that failed Primary Batch will be included in the eftpos Batch Settlement on the next RITS Business Day.

8.11.4 FTS Event procedure where there is only one DSEP

If an FTS Event occurs, the following procedure will be followed.

a. **Suspension of Member**: Rule 14 of the Scheme Rules applies and the DSEP's participation may be suspended so that no further Settlement obligations will arise from new eftpos Transactions initiated by the DSEP's customers, if an Issuer, or accepted by the DSEP or its customers, if an Acquirer. Such suspension does not relieve the DSEP from the obligation to discharge any existing Settlement obligations.

b. **Options for the Company**: Further Settlement of eftpos Transactions pursuant to the eftpos Scheme Rules and/or these Technical Operational and Security Rules may be deferred in accordance with clause 8.11.2 or suspended or be performed in accordance with this clause 8.11.4(c) to (g) by notice from the Company.

c. **Procedure after an FTS Event**: As soon as practicable after an FTS Event occurs and provided Settlement is not deferred under clause 8.11.2 or suspended under clause 8.11.4(b), the Company will:

    i. notify all Members, the RBA and APRA of the occurrence of the FTS Event in respect of the DSEP and that changed Settlement arrangements in accordance with this clause 8.11.4 will be used for the eftpos Batch Settlement in respect of that DSEP for itself and all Indirect Settlers on behalf of whom it settles;

    ii. if a DSEP's participation has been suspended under clause 14.1 or 14.4 of the Scheme Rules:

    iii. specify all BINs and Acquirer IDs used by the DSEP;

    iv. direct Members to the FTS Guidelines requirements in respect of both connectivity and Settlement changes and timing;

    v. provide an estimate of the date and time for Settlement, including for submission of a revised RITS Instruction, which may be through:

        A. Primary Batch including the Direct Settler suffering the FTS Event in the case of an FTS Event which is a Statutory Management;

        B. a Secondary Batch and DSEP Batch in the case of an FTS Event other than an Insolvency Event on the same RITS Business Day according to the procedure in 8.11.4(c)(iv) if the FTS Event is known before 12 noon on the RITS Business Day, or on any subsequent RITS

Business Day according to the procedure in 8.11.4(c)(v) if the FTS Event is not known before 12 noon on the RITS Business Day; or

C. a Primary Batch (excluding the DSEP) in the case of an FTS Event which is an Insolvency Event other than a Statutory Management, and a DSEP Report to be settled bilaterally at the election of the Survivors in the case of an FTS Event which is an Insolvency Event other than a Statutory Management;

vi. do each of the following, if the FTS Event is known before 12 noon on the RITS Business Day, provided that the FTS Event is not an Insolvency Event:

A. give notice to Members that the Batch Participant Reports for each Member, the Batch Agency Reports from each Settlement Agent and Indirect Settler pairing will be superseded and recall the RITS Instruction for the Primary Batch for that RITS Business Day;

B. re-calculate the Batch Participant Reports for each Member and provide revised Batch Participant Reports to each Member for each of a Secondary Batch and a DSEP Batch;

C. re-calculate the Batch Agency Reports for each Settlement Agent and Indirect Settler pairing and provide revised Batch Agency Reports to each Settlement Agent and Indirect Settler pairing for each of a Secondary Batch and a DSEP Batch; and

D. re-calculate and submit by 2pm the revised RITS Instruction for a Secondary Batch and a DSEP Batch for the relevant RITS Business Day;

E. provide the revised Batch Participant Reports and Batch Agency Reports and submit the revised RITS Instruction for Settlement of eftpos Transactions for each of a Secondary Batch and a DSEP Batch in accordance with the Scheme Rules and these Technical, Operational and Security Rules on the same RITS Business Day; and

F. notify all eftpos Batch Participants when the RITS Instruction for the Secondary Batch and DSEP Batch have been submitted.

vii. do each of the following, if the FTS Event is not known before 12 noon on the RITS Business Day, provided that the FTS Event is not an Insolvency Event:

A. give notice to Members that the Batch Participant Reports for each Member, the Batch Agency Reports for each Settlement Agent and Indirect Settler pairing will be superseded and recall the RITS Instruction for the Primary Batch for that RITS Business Day;

B. re-calculate the Batch Participant Reports for each Member and provide revised Batch Participant Reports to each Member for each of a Secondary Batch and a DSEP Batch, together with Clearing Interest from that RITS Business Day to the next RITS Business Day;

C. re-calculate the Batch Agency Reports for each Settlement Agent and Indirect Settler pairing and provide revised Batch Agency Reports to each Settlement Agent and Indirect Settler pairing for each of a Secondary Batch and a DSEP Batch, together with Clearing Interest from that RITS Business Day to the next RITS Business Day; and

D. re-calculate and submit on the next RITS Business Day a revised RITS Instruction for a Secondary Batch and a DSEP Batch, together with Clearing Interest from that RITS Business Day to the next RITS Business Day;

E. provide the revised Batch Participant Reports and Batch Agency Reports and submit the revised RITS Instruction for Settlement of eftpos Transactions for each of a Secondary Batch and a DSEP Batch in accordance with the Scheme Rules and these Technical, Operational and Security Rules on the same RITS Business Day; and

F. notify all eftpos Batch Participants when the RITS Instruction for the Secondary Batch and DSEP Batch have been submitted in accordance with clauses 8.4 to 8.6 above as if the Secondary Batch and DSEP Batch were the Primary Batch on the next RITS Business Day;

viii. if the FTS Event is an Insolvency Event other than Statutory Management:

A. give notice that the Batch Participant Reports for each Member, the Batch Agency Reports for each Settlement Agent and Indirect Settler pairing will be superseded and recall the RITS Instruction for the Primary Batch for that RITS Business Day;

B. re-calculate the Batch Participant Reports for each Member that is a Survivor and provide revised Batch Participant Reports to each Member that is a Survivor for a revised Primary Batch (excluding the DSEP suffering an Insolvency Event), together with Clearing Interest for each calendar day until the RITS Business Day on which Settlement is to occur;

C. re-calculate the Batch Agency Reports for each Settlement Agent that is a Survivor and Indirect Settler pairing and provide revised Batch Agency Reports to each Settlement Agent that is a Survivor and Indirect Settler pairing for a revised Primary Batch (excluding the DSEP suffering an Insolvency Event) together with Clearing Interest for each calendar day until the RITS Business Day on which Settlement is to occur; and

D. re-calculate and submit on the earliest possible RITS Business Day a revised RITS Instruction for all Survivors, for a revised Primary Batch (excluding the DSEP suffering an Insolvency Event), together with Clearing Interest for each calendar day until the RITS Business Day on which Settlement is to occur; and

E. notify all eftpos Batch Participants when the RITS Instruction for a revised Primary Batch (excluding the DSEP suffering an Insolvency Event) has been submitted in accordance with clause 8.4 to 8.6 above on the next RITS Business Day; and

F. calculate for and provide a DSEP Report to each Survivor and the DSEP for Settlement obligations of each Survivor against the DSEP on a bilaterally netted basis for bilateral Settlement.

d. **Non Insolvency Event procedure for subsequent RITS Business Days:** For each RITS Business Day after the day on which an FTS Event occurs (for an FTS Event that is not an Insolvency Event) until a DSEP ceases to be a DSEP or is removed as a Member, the Company will:

i. calculate and provide to each Member the Batch Participant Report for that Member for a Secondary Batch and a DSEP Batch;

ii. calculate and provide to each Settlement Agent and Indirect Settler the Batch Agency Report for that Settlement Agent for a Secondary Batch and a DSEP Batch;

iii. calculate and submit on the next RITS Business Day a RITS Instruction for a Secondary Batch and a DSEP Batch; and

iv. notify all eftpos Batch Participants when the RITS Instruction, for that RITS Business Day in accordance with clauses 8.1 to 8.10 above as if the Secondary Batch and DSEP Batch were the Primary Batch.

e. Insolvency Event (other than Statutory Management) procedure for subsequent RITS Business Days: For each RITS Business Day from and after the day on which an FTS Event which is an Insolvency Event other than a Statutory Management occurs until the DSEP is terminated as a Member:

i. the DSEP is excluded from eftpos Batch Settlement; and

ii. the Company will prepare a cumulative DSEP Report for all outstanding Settlement obligations of the DSEP against each Survivor netted on a bilateral basis.

f. **Statutory Management procedure for subsequent RITS Business Days:** For each RITS Business Day from and after the day on which an FTS Event which is a Statutory Management occurs and whilever the DSEP remains under Statutory Management and the Company has not suspended or terminated the DESP's participation, the DSEP remains part of or returns to being part of the Primary Batch. If a Statutory Management ceases and the DSEP remains an eftpos Member then clauses applying to an FTS Event that is an Insolvency Event apply.

g. **Procedure post Member being removed**: When a DSEP ceases to be a DSEP or is removed as a Member, Settlement will revert to the use of the Primary Batch procedure in accordance with clauses 8.1 to 8.10 above.

8.11.5 Responsibility for Settlement following an FTS event

a. Unless the FTS Event is an Insolvency Event, each eftpos Batch Participant that is a Survivor and a net payer (either directly or through their Settlement Agent) will:

i. where the FTS Event is known before 12 noon on a RITS Business Day, by 4pm on that RITS Business Day, ensure that there are sufficient funds in their ESA to discharge the Settlement obligations of that eftpos Batch Participant (including those of any Indirect Settlers or Non-clearers on whose behalf it Settles) for the purposes of each of the Secondary Batch and DSEP Batch; or

ii. where the FTS Event is not known before 12 noon on a RITS Business Day and Settlement is deferred to the next RITS Business Day, by 8:45am on the next RITS Business Day, ensure that there are sufficient funds in their ESA to discharge the Settlement obligations of that eftpos Batch Participant (including any Indirect Settlers or Non-clearers on whose behalf it Settles) for the purposes of each Secondary Batch and DSEP Batch to be run on that next RITS Business Day.

b. Where a Member becomes a DSEP and Settlement with the DSEP through the Primary Batch is recalled by the Company, Survivors and the DSEP must discharge any Settlement obligations in respect of eftpos Transactions that occurred before the FTS Event using the Batch Participant Reports prepared for the Secondary Batch and DSEP Batch.

c. If the FTS Event is an Insolvency Event (other than statutory management), each Survivor must determine with an authorised representative or administrator of the DSEP the manner in which that Survivor and the DSEP will fulfil Settlement obligations for any then outstanding eftpos Transactions between them, provided that any such Settlement will be on a bilateral and net basis between the DSEP and each Survivor using the netted Settlement obligations calculated in the DSEP Report.

d. If the DSEP is a Settlement Agent for other Members or Non-clearers:

i. the Settlement Agent (or their administrator under an Insolvency Event) must notify each Member and Non-clearer on behalf of whom the DSEP settles of the occurrence of an FTS Event in respect of the DSEP and to invoke their contingency Settlement arrangements;

ii. each impacted Member must invoke their contingency Settlement arrangements and notify the Company of their alternative Settlement Agent as soon as practicable after the Member if notified by the Settlement Agent or by the Company of the FTS Event; and

iii. the Company will continue to include Settlement obligations for all Members and Non-clearers using that DSEP as a Settlement Agent within that DSEP's DSEP Batch until the Company is notified of an alternative Settlement Agent for the relevant Member or Non-clearer.

e. For clarity, only existing eftpos Batch Participants are able to be Settlement Agents for Indirect Settlers.

f. Neither the Company nor any other Survivor has any liability in respect of unsatisfied Settlement obligations or Losses arising as a result of one or more Members suffering an FTS Event or Potential FTS Event, except as expressly stated in the eftpos Scheme Rules, these Technical, Operational and Security Rules.

g. For the avoidance of doubt, neither the occurrence of an FTS Event nor the Survivor's election to Settle bilaterally with the DSEP:

   i. extinguishes or abrogates the DSEP's Settlement obligation in respect of eftpos Transactions that occurred before an FTS Event or the time of suspension of the DSEP's participation; or

   ii. extinguishes or relieves a Survivor's Settlement obligation in respect of eftpos Transactions that occurred before an FTS Event or the time of suspension of the DSEP's participation.

8.11.6 Consequences of use of Secondary Batch and DSEP Batch

If the Company uses a Secondary Batch and DSEP Batch, the following possible consequences may occur:

a. both the Secondary Batch and the DSEP Batch settle prior to the close of the RITS Business Day. In this case, the DSEP will no longer be a DSEP and the Company will revert to a Primary Batch for the next RITS Business Day;

b. the Secondary Batch settles but the DSEP Batch does not settle. In this case:

   i. Settlement Obligations of each Survivor against the DSEP will continue to be separately netted from the netted Settlement Obligations between the Survivors;

   ii. the Settlement obligations under the failed DSEP Batch will be carried over into the next DSEP Batch, which will show outstanding Settlement obligations, new Settlement obligations and extra Clearing Interest on the outstanding Settlement obligations for the number of days since the last time that a batch including the DSEP settled. The outstanding Settlement obligations will have a different number of days Clearing Interest applied from any new Settlement obligations.;

   iii. the calculation and provision of Batch Participant Reports, Batch Agency Reports and RITS Instructions for the DSEP Batch will continue to be prepared for each subsequent RITS Business Day in accordance with clause 8.11.6(b)(ii) above until either:

      A. the DSEP Batch settles and the DSEP ceases to be a DSEP; or

B. the DSEP's membership is terminated and all their Settlement obligations are extinguished;

c. the DSEP Batch settles and the Secondary Batch does not settle (without an FTS Event occurring). In this case, the DSEP will cease to be a DSEP and Settlement will occur using a Primary Batch in accordance with clauses 8.1 to 8.10 above, including any outstanding Settlement obligations carried over from the failed Secondary Batch, together with extra Clearing Interest on the outstanding Settlement obligations for the number of days since Settlement last occurred before the creation of the Secondary Batch. The outstanding Settlement obligations will have a different number of days Clearing Interest applied from any new Settlement obligations;

d. the DSEP Batch settles and the Secondary Batch does not settle (because of FTS Event occurring for another Direct Settler). In this case, the DSEP will cease to be a DSEP but clause 8.11 will be applied in respect of the new DSEP; or

e. neither the Secondary Batch nor the DSEP Batch settle. In this case:

   i. all outstanding Settlement obligations under each of the failed Secondary Batch and the failed DSEP Batch will be carried over to each of the Secondary Batch and the DSEP Batch for the next RITS Business Day, together with extra Clearing Interest on the outstanding Settlement obligations for the number of days since Settlement last occurred. The outstanding Settlement obligations will have a different number of days Clearing Interest applied from any new Settlement obligations;

   ii. the calculation and provision of Batch Participant Reports, Batch Agency Reports and RITS Instructions for each of the Secondary Batch and the DSEP Batch will continue to be prepared for each subsequent RITS Business Day in accordance with clause 8.11.6(e) (i) above until any of the above sub-clauses happen.

8.12. Systemic FTS if there is more than one DSEP

If there is more than one DSEP in the Primary Batch as at 12 noon, Clause 8.11.2 will apply as if the references to "DSEP" were a reference to all DSEPs (as in the case of a systemic FTS there will be more than one DSEP). However, if Settlement is deferred continually for more than 3 RITS Business Days, at the direction of the Company in consultation with the RBA and APRA, Direct Settlers must discharge their Settlement obligations within 3 Business Days using the RBA's Real Time Gross Settlement system or according to such other timing or method as agreed between the impacted Direct Settlers, outside of the eftpos Batch Settlement.

9. Reporting

9.1. Member reporting to the Company

9.1.1 eftpos Transaction data

All Members are to report their eftpos Transaction data (including Off-Us Transactions and On-Us Transactions) to the eftpos Hub service provider, in the form of a Member Batch File in accordance with the eftpos Hub Files and Reports – POS Specification.

This data and Transaction data generated by the eftpos Hub enables the Company to perform various governance and analytics activities, including to evaluate the performance of the eftpos Payment System, Member compliance with the Scheme Rules and these Technical, Operational and Security Rules, for product development and support or to provide services to Members or respond to a direction or authority from an eftpos Consumer to disclose Transaction data and history to an authorised third party (provided Personal Information and the source of the data are not disclosed except to the Member from which the information was received or in accordance with any eftpos Consumer authority or consent).

From 20 October 2020, Members must report all eftpos Transactions confirmed as fraud or scams:

a. Where Members are reporting eftpos Transactions confirmed as fraud or scams directly to AFCX, eftpos shall retrieve a copy of such reports from AFCX, and such Members are not required to separately transmit such reports to eftpos.

b. Where Members are not reporting eftpos Transactions confirmed as fraud or scams directly to AFCX, Members shall transmit to eftpos a daily report of eftpos transactions confirmed as fraud or scams, using the AFCX CF format.

c. This includes all disputes raised by an Issuer under Reason code 30101 - Card Not Present Fraud

The Company will use this data for, for example:

a. Calculation of Member voting entitlements;

b. Calculation and billing of eftpos Scheme fees;

c. Calculation and billing of any other fees payable to the Company;

d. Transaction analytics to support the strategic objectives and product development of the Company and its Members;

e. Provision of Regulatory reporting by the Company;

f. Assessment of Member compliance obligations;

g. Reporting of Fraud Transactions occurring on the network; and

h. Reporting of Transactions where customers claim they are a victim of a scam.

For batch reporting, Members must report once per calendar day at the end of the calendar day unless the Member and the Company have agreed that the Member may transmit multiple files throughout the day due to excessive file size. Refer to the Standard Hub Service Schedule for batch file reporting and delivery requirements by Direct Connectors to the eftpos Hub.

Transactions are reported once they are complete. That is, both the request and the response are sent and received for each Transaction.

Off-Us transactions and On-Us transactions	**Successful**	**Unsuccessful (declined)**	**POS Channel**	**Online Channel**	**Mobile Channel**	**ATM Channel (where applicable)**
0200 / 0210 = > 9200						
Includes (where supported by channel): • Purchase • Purchase with Cashout • Cashout • Refund • Deposit • Withdrawal • Short Duration Pre-Authorised Transaction For Members receiving ATM processing services: • ATM Withdrawal • ATM Deposit • ATM Balance Enquiry	Conditional (i.e. Mandatory if not reversed Optional if reversed)	Mandatory	Yes	Yes	Yes	Yes
0220 / 0230 = > 9220						
Financial advice (including Fallback Transactions)	Conditional (i.e.	Mandatory	Yes	No	Yes	No

Off-Us transactions and On-Us transactions	Successful	Unsuccessful (declined)	POS Channel	Online Channel	Mobile Channel	ATM Channel (where applicable)
	Mandatory if not reversed Optional if reversed)					
0420 / 0430 = > 9420						
Reversal	Conditional (i.e. for all with financial transactions)	Mandatory	Yes	Yes	Yes	Yes

Table 9: Transactions to report

Members are not required to report transactions that are:

a. Network management messages;

b. Reconciliation messages; and

c. Administrative messages.

9.1.2 Member Monthly Reporting

Acquirer Members and Issuer Members are to provide the Company with a Member Monthly Report within 15 calendar days of the end of each calendar month. The Monthly Member Report must contain the information as set out in Clause 9.1.2.1 and Clause 9.1.2.2 and Appendix 2A. Where there is a discrepancy between the requirements stipulated in Clause 9.1.2.1 and Clause 9.1.2.2 and Appendix 2A, completion of the report in Appendix 2A will satisfy these requirements.

9.1.2.1 Issuer reporting

Each Issuer Member must, for that Issuer Member and each Non-clearer represented by them, report to the Company the following information for the period since the last report provided by the Issuer Member to the Company:

a. Relating to eftpos Form Factors that are cards, in each case specifying if the card is a new issue or replacement issue:

  i. total numbers of cards on issue (including Multi-Network Cards);

  ii. total numbers of cards on issue which are capable of being used for eftpos Transactions only;

b. total Chip Cards on issue;

  i. total Chip Cards on issue that are capable of being used for eftpos Transactions only;

  ii. total contact only Chip Cards on issue;

  iii. total dual interface Chip Cards on issue;

  iv. total dual interface Chip Cards on issue that are capable of being used for eftpos Transactions only;

  v. total number of Active Cards by card type;

c. relating to any eftpos Form Factor that is not a card, in each case specifying if the eftpos Form Factor is encompassed within a method provided or enabled by the Issuer Member solely or in conjunction with another entity:

  i. total numbers of eftpos Consumers enabled for the eftpos Form Factor;

  ii. where the Company is not the TSP, the total number of Payment Tokens issued, including as a sub-set the total number of Payment Tokens issued relating to Multi-Network Cards; and

d. for all eftpos Form Factors:

  i. any incompatibility or security issues raised by entities other than the Company; and

  ii. any directions that the Member receives from another person which is contrary to a regulatory position published by the Reserve Bank of Australia.

9.1.2.2 Acquirer reporting

Each Acquirer Member and Self-Acquirer must report to the Company following information:

a. total numbers of eftpos Terminals deployed;

b. total numbers of eftpos Terminals deployed capable of accepting eftpos Form Factors which are Chip Cards;

c. total numbers of eftpos Terminals deployed configured to accept eftpos Form Factors which are Chip Cards;

d. total numbers of eftpos Terminals deployed configured to accept eftpos Form Factors other than eftpos Chip Cards;

e. total numbers of eftpos Terminals deployed configured to route transactions through the eftpos Payment System as a priority;

f. total number of Authorised eftpos Digital Merchants;

g. No longer used

9.1.3 Monthly Interchange reporting

For future use

9.1.4 Disputed Transactions and Chargebacks reporting

For future use.

9.1.4.1 No longer used

9.1.5 Merchant reporting

9.1.5.1 All Merchants

Refer to Clause 7.8 for Chargeback monitoring reporting requirements.

9.1.5.2 Authorised eftpos Digital Acceptance Merchants

Refer to Clause 4.17 for Fraud reporting requirements.

9.1.6 Service Level reporting and Force Majeure

Within 10 Business Days of the end of each calendar month, each Direct Connector must for itself and for each Member, eftpos Issuer, eftpos Acquirer, Direct Settler and Non-clearer for which it provides services, provide to the Company a report for the immediately preceding calendar month indicating whether or not the Direct Connector met the service levels for its Standard Direct Connection Service.

If the Direct Connector did not meet the required service levels, the Direct Connector must identify the service level and indicate the level achieved, the difference between the required service level and the level achieved, the last three calendar month's view of performance by the Direct Connector and include any explanation of the deficiency against service level, steps being taken by the Direct Connector or which may be required by another Direct Connector to change systems or processes to achieve the service levels and an estimate of the timing of when the services are likely to be reinstated to required levels.

A Member impacted by a Force Majeure Event must:

a. immediately notify the Company and describe the nature of the Force Majeure Event and its likely effect on performance of its obligations in respect of a Direct Connection;

b. use commercially reasonable endeavours to continue or resume performance without delay, including by means of alternate resources, workarounds or other means; and

c. keep the Company informed of progress and expected restoration of the Direct Connection to required service levels.

9.1.7 Reports of Notifiable Incidents

Each Member must notify to the Company, at a telephone number or email nominated from time to time by the Company, the occurrence of a Notifiable Incident event impacting eftpos Consumers or Merchants within 1 hour of the breach being identified. The notifying Member must follow the procedure and report the information required by Clause 9.1.7.1 and Clause 9.1.7.2 below.

9.1.7.1 Notifiable Incident post incident procedure

The Company or any notifying Member must follow the procedure set out below:

a. take immediate steps to cease the unauthorised access and minimise future incidents of the same type:

b. investigate any known Notifiable Incident as a matter of urgency and in any event:

c. complete an expeditious assessment of the Notifiable Incident, including possible impacts of the Notifiable Incident and likelihood of harm to individuals to whom the Personal Information relates within 3 calendar days;

d. provide impacted parties with reasonable ongoing updates on the results of the investigation and assessment at a frequency which reflects the severity of the Notifiable Incident and until remediation efforts are completed and prevention plans in place;

e. provide reasonable assistance to impacted parties for their investigations, assessment and management of the Notifiable Incident; and

f. cooperate with all impacted parties required to report the Notifiable Incident to applicable regulators and/or impacted individuals (as applicable);

g. agree with the Member (in the case of the Company) and with the Company (in the case of a Member) the manner, form and timing (subject to any requirements of Law) of communication by each party to regulators and any impacted eftpos Consumers or Merchants in respect of the Notifiable Incident;

h. co-operate fully with any relevant law enforcement agency in relation to the data breach or compromise;

i. where requested by the Company, commence or co-operate with the Company in the conduct of a Root Cause Analysis, within 21 days of the occurrence of a confirmed Notifiable Incident, to determine, among other things:

   i. details referred to in the report section below;

   ii. systems impacted;

   iii. source of the unauthorised access;

   iv. perpetrator of unauthorised access;

   v. whether any additional parties were involved in the unauthorised access;

j. commence a compliance evaluation of the eftpos Hub and any relevant Direct Connection with Laws and Technical, Operational and Security Rules within 35 days of the data breach or compromise using reputable, experienced and independent auditors and notify other impacted parties of the progress of such evaluations; and

k. provide a copy of the results of the Root Cause Analysis with impacted parties and, where necessary, relevant regulators.

9.1.7.2 Notifiable Incident post incident report

For each Notifiable Incident notified to the Company under Clause 9.1 or by the Company under Clause 9.2, the entity whose systems, Service Provider or Merchant was the source of such Notifiable Incident must report to the Company (or if the Company is notifying of a Notifiable Incident to impacted Members) the following (or as much as is then known at the time for the relevant report), initially within 24 hours after the Notifiable Incident is identified and keep the Company updated on developments and the remediation plan until all remediation activities have been completed:

a. nature of the Notifiable Incident;

b. source of the breach or compromise;

c. the name of any contributing Service Provider;

d. the nature and type of information compromised or subject to unauthorised access;

e. the number of eftpos Form Factors impacted or at risk by the data breach or compromise;

f. the Members whose eftpos Consumers were impacted by the data breach or compromise and numbers of eftpos Form Factors per impacted Member;

g. whether and the timing of any notifications given by the Member to regulator(s) and other Members and the names of the regulators and Members notified;

h. the number and value of fraudulent Transaction claims made by or against the Member's eftpos Consumers for Transactions that occurred during the period to which the data breach or compromise applied (whether eftpos Consumers or Merchants);

i. the remediation activities and rectification plan for the data breach or compromise or the steps undertaken by the Member to rectify the data breach or compromise, where rectification has been completed as at the date of the report;

j. whether and the number and dates of previous data breaches or compromises (reported or not) of the same type or involving the same contributing Service Provider(s) or Merchants;

k. in the case of the Company for the eftpos Hub, impacted Members;

l. the steps taken to stop the unauthorised access to the information;

m. the steps taken to prevent any future compromises of the same or a similar type;

n. the steps taken to recover or rectify any compromised information;

o. the proposals to notify impacted parties, including recommendations about the steps to be taken by any impacted individuals and the method for provision of notification, and the proposal to notify any regulator; and

p. the proposals to remediate or mitigate the impact to eftpos Consumers and Merchants.

9.1.8 Transaction security requirements – transmission and storage

The sensitive information of each Transaction must be protected both during transit and storage in accordance with AS 2805 and PCI-DSS requirements and delivery of Member Batch Files must be protected in accordance with the eftpos Hub Files and Reports – POS Specification.

9.1.9 Access

Transactional data must be protected from unauthorised access, such as by data protection at the database level (e.g. password/access list).

9.2. Reporting by the Company

9.2.1 eftpos Transaction reporting

After the end of each calendar month, the Company will make available to each Member an eftpos Transaction Report, which forms part of the fees invoice issued by the Company containing the following information for the relevant Member and all eftpos Issuers, eftpos Acquirers, Direct Settlers and Non-clearers represented by that Member:

a. the number of each Off-Us Transaction type acquired by that Member during the calendar Month with each Issuer Member with whom it directly settles;

b. as extracted from the daily Member Batch File, the number of each On-Us Transaction type acquired by that Member during the calendar Month; and

c. the number of each Off-Us Transaction type performed by customers of that Member during the calendar month with each Member with whom it directly settles.

This does not supersede the requirement for Members to provide a daily Member Batch File in accordance with Clause 9.1. The format for the eftpos Transaction Report will be provided together with the Direct Connector On-boarding Pack for Direct Connections to the eftpos Hub.

9.2.2 Service Level reporting

After the end of each calendar quarter, the Company will provide to each Member utilising a Direct Connection to the eftpos Hub, a report for the immediately preceding calendar quarter indicating whether or not the Company met the service levels for the eftpos Hub.

Where a Force Majeure Event impacts the eftpos Hub, the Company will notify Direct Connectors and Members of progress and expected restoration of the eftpos Hub to required service levels.

9.2.3 Reports of unauthorised access to Consumer data

The Company will as soon as reasonably practicable, notify each impacted Member if the Company becomes aware or suspects that a data breach or compromise has been or is likely to be caused by the eftpos Hub.

The Company must then follow the procedure and provide the information (as far as is known by the Company) set out in clause 9.1.7.

The Company will also notify impacted individuals and relevant regulators of any data breach or compromise has been or is likely to be caused by the eftpos Hub in accordance with applicable Law.

9.3. Disclosure

The Company may disclose the Transaction and Disputed Transactions and Chargebacks information provided pursuant to Clause 9.1:

a. to any party and in any manner authorised by the Scheme Rules;

b. in the case of eftpos Mobile using an ESE, and only in respect of eftpos Cards Provisioned to their relevant devices, to the OEM for the relevant device

c. on the basis of confidentiality agreements, to one or more service providers engaged by the Company for the purposes of conducting Transaction analytics and for the Company's other internal business purposes;

d. on an aggregate basis across all Members or Merchants or Transaction types or in any other segmentation, to one or more Members for that Member's internal business purposes; and

e. on an aggregate basis across all Members or Merchants or Transaction types or in any other segmentation, as required by Law, to a regulator or, together with transaction analysis or interpretation, in press releases, media responses and other public documents issued by the Company.

The Company may use and disclose the Notifiable Incident information provided by a Member pursuant to Clause 9.1 above, excluding any eftpos Consumer or Merchant Personal Information, to any party and in any manner authorised by the Scheme Rules.

Appendix A. Definitions and interpretations

Terms used in these Technical, Operational and Security Rules not defined in this Clause have the meanings given to the in the eftpos Scheme Rules.

Section 1.2 Schedule 1 of the eftpos Scheme Rules applies to these Technical, Operational and Security Rules.

Defined Term	eftpos Definition
Acceptance Device	has the meaning in the Scheme Rules.
Account Verify Request (AVR)	is a non-financial message which will verify that the eftpos Form Factor is valid, has not been cancelled, or reported lost or stolen at the time of the Account Verify message response. For clarity, this message does not verify available funds.
ACe	is the name given to any eftpos integrated circuit (i.e. chip) application certified by the eftpos Certification Body as compliant with the eftpos card specifications published by eftpos from time to time.
Acquirer	has the same meaning as eftpos Acquirer and Acquirer member.
Acquirer Member	has the meaning in the Scheme Rules.
Acquirer Identification Number (AIN)	means a unique number allocated to the Acquirer for identification purposes by the International Organisation for Standardisation (ISO). Where the Acquirer is also an Issuer, the member's BIN allocated in relation to its proprietary debit cards may be utilised as the member's Acquirer Identification Number.

Defined Term	eftpos Definition
Acquirer's End of Day	means the time when the last of the Acquirer's Interchange Link to the eftpos Hub has been cutover to the next Transaction Settlement Date, whether by the Acquirer or by the eftpos Hub.
Acquiring Token	has the meaning as in the PCI Tokenization Product Security Guidelines, that is a value that replaces a PAN. An Acquiring Token may be any format including (for example, an alphanumeric string, or a 13-19 digit numeric value in a designated BIN range). For clarity, an Acquiring Token may, but need not, also meet the definition of a Payment Token. Acquiring Tokens must not have the same value as or conflict with a real PAN.
Active Card	means an eftpos Card used within the 30 day period immediately preceding the date of the report.
AID	means application identifier, the unique code associated with a smart card application, which allows the Terminal to select a suitable application within the card for a given operation. The AID is based on a registered number in accordance to ISO 7816-5 standards. The permitted AIDs for the eftpos card debit scheme are the following: a. A00000038410: eftpos Savings b. A00000038420: eftpos Cheque
Application	defines chip data elements specific to an AID. A chip application specifies the card usage (e.g. online-only usage, online with offline capability usage, etc.) depending on the risk model (debit card, credit card, ATM-only card, etc.) defined by the Issuer.
Application Authentication Cryptogram (AAC)	an application cryptogram that the Chip card generates to indicate that the transaction has been declined offline because of either the rejection of that specific transaction or a restriction that does not allow the use of the card in that environment.
Application Cryptogram (AC)	a cryptogram that is generated and returned by the Chip card. The three types of cryptograms are the Transaction Certificate (TC);

Defined Term	eftpos Definition
	Authorisation Request Cryptogram (ARQC); and Application Authentication Cryptogram (AAC).
Application Response Cryptogram (ARPC)	an application cryptogram generated by the Issuer and used by the card to verify that the response came from the Issuer.
Application Request Cryptogram (ARQC)	an application cryptogram that the Chip card generates to indicate that the transaction must go online to the Issuer for authorisation.
Application Selection Indicator (ASI)	an application cryptogram that the eftpos Chip card generates to indicate that the transaction must go online to the Issuer for authorisation.
Application Transaction Counter (ATC)	a counter maintained by the application in the EMV chip card. Incrementing the ATC is managed by the EMV chip card.
APRA	means Australian Prudential Regulation Authority
Approved Digital Acceptance Solution	A solution notified by the Company from time to time via Member Advice.
AS	means Australian Standard as published by Standards Australia.
AusPayNet CNP Framework	means the CNP Fraud Mitigation Framework published from time to time by the Australian Payments Network
Australian IC Card	means an IC card in respect of which the EMV Issuer Country Code data element (tag 5F28) is equal to "036" (Australia).
Australian Payments Network	has the meaning in the Scheme Rules.

Defined Term	eftpos Definition
Australian Payments Network SCD Letter of Approval	means a letter, issued by the Australian Payments Network, certifying that a Secure Cryptographic Device has been approved for use within the IAC Code Set.
Authentication	means the act of confirming the truth of an attribute of a datum or entity.
Authorisation	in relation to an eftpos Transaction, means confirmation given by an Issuer that funds will be made available for the benefit of an Acquirer to the amount of that Transaction. Except in the circumstances specified in these Rules, Authorisation is effected online. Issuer confirmation may also be delegated to the EMV chip when processed as an offline authorisation.
Authorised	has the same meaning as Authorisation.
Authorised Device	means a Secure Cryptographic Device that has been approved in accordance with clause 4.3 of these Rules.
Authorised eftpos Digital Merchant	has the meaning in the Scheme Rules.
Available	has the meaning in the Scheme Rules.
Bank Identification Number (BIN)	has the meaning in the Scheme Rules.
BIN Controller	means an entity that governs PAR and ensures PAR uniqueness within its own ecosystem that falls under its span of control.
Batch Agency Report	means a report for each Direct Settler and Indirect Settler pairing for their netted position.
Batch Participant Report	means a report of the netted position of a eftpos Batch Participant (including any Indirect Settler on whose behalf they

Defined Term	eftpos Definition
	Settle) against each other eftpos Batch Participant (including any Indirect Settler on whose behalf they Settle).
Batch Recorded Date	means: a. the Transaction Settlement Date if that date is the same as a RITS Business Day; or b. the next RITS Business Day if the Transaction Settlement Date is not a RITS Business Day
Business Application Indicator (BAI)	means the merchant/gateway business application type that allows eftpos and its Members to apply applicable rules for transaction processing
Card	has the same meaning as eftpos Card.
Card Authentication Method (CAM)	a method to determine if a card is valid. Examples include but are not limited to: Chip CVN, CVN2, DDA/CDA, AC.
Card-Not-Present (CNP)	has the meaning in the Scheme Rules.
Card on File (CoF)	means Card credentials stored at a Merchant or Merchant Service Provider used when an eftpos Consumer registers their eftpos Form Factor with the Merchant for use in future purchases of goods or services from that Merchant.
Card Sequence Number	refers to issuer sequence number
Card Standards	means, in relation to Cards, the standards from time to time included in clause 3.2 of these Rules.
Card Verification Value (CVV)	means card verification value and forms part of the message format.

Defined Term	eftpos Definition
Cardholder	has the same meaning as eftpos Consumer as defined in the Scheme Rules.
Cardholder Authentication	means the process of validating the individual providing payment Card details is the rightful owner of those Card details and that the Card account is current and in good standing. Cardholder Authentication may be independent of any payment transaction and must be performed prior to granting an Acquiring Token or a service being approved in accordance with the eftpos CNP Standard capturing Card details for use in subsequent transactions. Cardholder Authentication may be conducted at the point of initiation of an eftpos Digital transaction using either a Risk Based Analysis or a Strong Customer Authentication method.
Cardholder Initiated Transaction	has the meaning in the Scheme Rules.
Cardholder Verification Method (CVM)	the verification method which the card and Terminal agree should be used for a particular transaction e.g. Offline PIN, Online PIN or Signature. The CVM list is encoded onto a Chip Card at the time of personalisation.
Cash	means Australian legal tender in circulation.
Cashout	has the meaning in the Scheme Rules.
Certificate	means a public key that has been digitally signed by a trusted authority to identify the user of a public key.
Certification	has the meaning given in the Scheme Rules.
Certification Checklist	has the meaning given in the Scheme Rules.

Defined Term	eftpos Definition
Chargeback	means the process by which the value of a Disputed Transaction is passed back from the Acquirer to the Issuer.
Chip	An integrated circuit designed to perform processing or memory functions.
Chip card	A card embedded with chip that communicates information to an eftpos Terminal.
Chip Fallback	A transaction where the authorisation is delegated to the card's Chip when the transaction is unable to be processed online.
Clearing Interest	means, unless a contrary intention is expressly stated, the interest calculated, at the rate payable by the RBA on overnight credit balances of Exchange Settlement Accounts held with the RBA (referred to as "ESR" by the RBA), for the period between the Batch Recorded Date of an eftpos Transaction and the RITS Business Day on which Settlement occurs. The rate applied is always the rate that is in effect on the day of the batch run, even if some Settlement obligations relate to a prior period.
Cloud Based Payments Solution or CBP Solution	means a solution that uses contactless NFC functionality to perform an eftpos Transaction following Provisioning of an eftpos Form Factor to a Mobile Device. For clarity, an OEM Solution is not a Cloud Based Payment Solution.
CNP Fraud Rate	means the aggregate of fraudulent transactions as calculated for Issuers and Merchants in accordance with AusPayNet CNP Framework.
CNP Fraud Threshold	means the maximum allowable Issuer or Merchant Fraud Rate as published in the AusPayNet CNP Fraud Framework.
COIN	has the meaning in the Scheme Rules.

Defined Term	eftpos Definition
COIN Operating Manual	has the meaning in the Scheme Rules.
Combined Dynamic Data Authentication (CDA)	means a CAM whereby a Terminal performs a cryptographic validation of a digital signature generated by the card at each transaction.
Company	means eftpos Payments Australia Limited, ABN 37 136 180 366.
Compromised Terminal	means a Terminal that has been tampered with for fraudulent purposes.
Consumer Disputed Transaction	a. means a transaction where an amount has been debited from the eftpos Consumer's account with their Issuer and the eftpos Consumer claims: b. The transaction was not initiated by the eftpos Consumer; c. The amount is incorrect; d. Purchased goods or services have not been received in full or at all; e. That the eftpos Consumer paid using another payment method; or f. That goods or services have been received but are not as described and the eftpos Consumer has not resolved the matter with the Merchant within 180 days from date of delivery of goods or services
Contactless Terminal Application Validation (cTAV)	Test methodology used by the eftpos Certification Body for contactless reader applications.
Contact Interface	defines the contact EMV application data elements.

Defined Term	eftpos Definition
CPoC	means the set of Contactless Payments on COTS requirements adopted and published from time to time by PCI Security Standards Council, LLC
Credentials	means in the case of eftpos Mobile, an eftpos Consumer's username and password which are required to be able to pay using eftpos Mobile.
Credit Items	includes all credit payment instructions, usually electronically transmitted, which give rise to eftpos interchange, except as may be specifically excluded by the Scheme Rules or these Technical, Operational and Security Rules.
Cryptogram	means the output from the process of transforming clear text into cipher text for security or privacy.
De-Tokenisation	means the process of retrieving a PAN value based on the Payment Token.
Debit Items	includes all debit payment instructions, usually electronically transmitted, which give rise to eftpos interchange, except as may be specifically excluded by the Scheme Rules or these Technical, Operational and Security Rules.
Deferred Card Present (DCP)	means a Transaction originating from an eftpos Form Factor being presented to an eftpos Terminal, which is not transmitted to the Issuer until a later time after the interaction between the eftpos Form Factor and the eftpos Terminal.
Deferred Payment	has the meaning in the Scheme Rules.
Deny List	means in relation to eftpos Open Loop Transit, a register of eftpos Form Factors which cannot be used to initiate a Purchase transaction for eftpos Open Loop Transit from time to time.

Defined Term	eftpos Definition
Digital Acceptance Device	has the meaning in the Scheme Rules.
Digital Fraud Rate	means the ratio of Chargebacks under the fraud reason code to approved eftpos Digital transactions.
Digital Wallet	A mobile application, website or other electronic facility that can be used by an eftpos Consumer for storing payment card details.
Direct Connection	has the meaning in the Scheme Rules.
Direct Connector	has the meaning in the Scheme Rules.
Direct Settler	has the meaning in the Scheme Rules.
Dispute Reason Codes	means the reason codes set out in the Disputed Transactions and Chargebacks Guide.
Disputed Transaction	Means: a. A Consumer Disputed Transaction; or b. An Issuer Disputed Transaction.
Disputed Transactions and Chargebacks Operations Guide	means the guide of that name as published by the Company from time to time.
Disputed Transaction Report	means the report, in the form specified by the Company from time to time, from Members of Disputed Transactions.
Disputed Transactions and Chargeback Form	means the form specified from time to time in the Disputed Transactions and Chargebacks Guide.

Defined Term	eftpos Definition
Disruptive Event	means any processing, communications or other failure of a technical nature, which affects, or may affect, the ability of Scheme Member to Interchange.
Domain Controls	means the checks eftpos will put in place to ensure that a transaction using eftpos Digital is only processed under the set of conditions approved by eftpos for the Acquiring Member submitting the transaction. This may include, but is not limited to Token Domain Restriction Controls.
Double Length Key	means a key length of 128 bits including parity bits or 112 bits excluding parity bits.
DSEP	means in relation to an FTS Event, a Direct Settler excluded from the Primary Batch which, prior to becoming a DSEP: a. fails to discharge Settlement obligations incurred by it (or any Indirect Settler or Non-clearer on behalf of whom it Settles) under or in accordance with the eftpos Scheme Rules and/or the Technical, Operational and Security Rules. This includes a failure to have sufficient funds in their ESA to settle their net Settlement obligation by 12 noon on the relevant RITS Business Day; or b. suffered an Insolvency Event, other than Statutory Management, in respect of itself; or c. is otherwise suspended or terminated pursuant to clauses 14 or 18 of the eftpos Scheme Rules.
DSEP Report	means a report of the Settlement obligations of each Survivor against the DSEP on a bilateral net basis.
Dynamic Data Authentication (DDA)	means a CAM whereby the Terminalperforms cryptographic validation of a digital signature generated by the chip card at each transaction.

Defined Term	eftpos Definition
eD+C	means the eftpos Disputed Transactions and Chargebacks workflow solution.
EFTPOS	means electronic funds transfer at point of sale.
eftpos or The Company	means the Company, eftpos Payments Australia Ltd.
eftpos Account	means an account of a type set out in clause 3.8(a)(ii) of these Technical, Operational and Security Rules.
eftpos Acquirer	means a Member which, in connection with an eftpos Transaction: a. on behalf of an eftpos Issuer, discharges the obligations owed by that eftpos Issuer to the relevant eftpos Consumer; and b. engages as a result in eftpos Interchange Activities with that eftpos Issuer.
eftpos API Gateway Services Schedule	means the document of that name as published by the Company from time to time.
eftpos API Specifications	has the meaning in the Scheme Rules.
eftpos Batch Settlement	has the meaning in the Scheme Rules.
eftpos Batch Participant	has the meaning in the Scheme Rules.
eftpos Card	has the meaning in the Scheme Rules.
eftpos Card Application Personalisation Specification (eCAPS)	means the document entitled eftpos Card Application Personalisation Specification published by the Company from time to time.

Defined Term	eftpos Definition
eftpos Card-Not-Present (CNP) Solution Assessment Criteria	has the meaning in the Scheme Rules. Formerly known as eftpos Digital Acceptance Framework (eDAF) Assessment Criteria.
eftpos Card-Not-Present (CNP) Standard	has the meaning in the Scheme Rules. Formerly known as eftpos Digital Acceptance Framework (eDAF) Acceptance Criteria Standard.
eftpos Cobrand Card	has the meaning in the Scheme rules
eftpos Consumer	has the meaning in the Scheme Rules.
eftpos Digital	has the meaning in the Scheme Rules.
eftpos Digital Acceptance	has the meaning in the Scheme Rules.
eftpos Digital Acceptance Framework Acceptance Criteria Standard	has the meaning in the Scheme Rules. Superseded by eftpos Card-Not-Present Standard.
eftpos Digital Acceptance Solution	has the meaning in the Scheme Rules. Formerly known as "Approved Digital Acceptance Solution", "Approved eftpos Digital Solution".
eftpos Digital Acceptance Solution Assessor Guide	has the meaning in the Scheme Rules. Superseded by eftpos Card-Not-Present Solution Assessment Criteria.
eftpos Form Factor	has the meaning in the Scheme Rules.
eftpos Hub	has the meaning in the Scheme Rules.

Defined Term	eftpos Definition
eftpos Hub Files and Reports Specifications	means each of the specifications issued by the Company from time to time setting out the required formats for files and reporting exchanged with the eftpos Hub, including: a. eftpos Hub Files and Reports – POS Specification; and b. eftpos Hub Files and Reports – ATM Specification.
eftpos Hub Link Specification (eLS)	has the meaning in the Scheme Rules.
eftpos In-App Payment	has the meaning in the Scheme Rules.
eftpos Interchange Activities	means the exchange of payment instructions and related messages between Members, usually by electronic means, in relation to eftpos Transactions.
eftpos Issuer	means a Member which issues an eftpos card and, in connection with any eftpos Transaction effected using that eftpos Card: a. assumes obligations to the relevant eftpos Consumer, which obligations are in the first instance discharged on its behalf by an eftpos Acquirer; and b. engages as a result in eftpos Interchange Activities with that eftpos Acquirer.
eftpos Mobile	has the same meaning in the Scheme Rules.
eftpos Mobile Service Schedule	means the document of that name as published by the Company from time to time.
eftpos Open Loop Transit	means the functionality which enables an eftpos Consumer with an eftpos Form Factor having eftpos Chip and Contactless capability, to initiate eftpos Transactions for a Transit Scheme. eftpos Open Loop Transit Transactions are processed using eftpos Terminals with eftpos Chip and Contactless capability.

Defined Term	eftpos Definition
eftpos Payment Token	a Payment Token which has been generated by the eftpos TSP.
eftpos Secure	has the meaning in the Scheme Rules.
eftpos Secure Directory Server	means the centralised connectivity, message transmission and authentication infrastructure, operated by or for the Company, for processing authentication requests and responses and for related eftpos Secure activities.
eftpos Secure Service Schedule	means the document of that name published by the Company from time to time.
eftpos Secure SCA User Experience Guide	means the document of that name published by the Company from time to time.
eftpos Secure Specifications	means the document of that name published by the Company from time to time.
eftpos Settlement Service	has the meaning in the Scheme Rules.
eftpos Terminal	has the meaning in the Scheme Rules.
eftpos Transaction	means an electronic funds transfer that: a. involves an eftpos Issuer and an eftpos Acquirer; b. and is processed via: i. an Interchange Link; and/or ii. processing infrastructure owned and operated by, or on behalf of, the Company; and c. is one of the transaction types described in the Scheme Rules.

Defined Term	eftpos Definition
eftpos Tokenisation Service for Tokens on File (eTS-F)	means the functionality which enables the tokenisation of card details as an eftpos Payment Token for Merchants to store on file for use in subsequent CNP eftpos Transactions.
eftpos TSP	means the applications operated by the Company for provision of Payment Tokens by the Company for eftpos Mobile and eftpos Digital.
eftpos TSP Service Schedule	has the same meaning as eTS-F Service Schedule
eQR Aggregator	Has the meaning in the Scheme Rules
eQR authenticated	Means eQR Pass Through Wallet transactions and transactions authenticated through 3DS where the authentication was performed during the payment
eQR unauthenticated	Means eQR transactions which are not considered Form Factor Present or 3DS transactions
eftpos QR (eQR)	Has the meaning in the Scheme Rules
eQR Pass Through Wallet (PTW)	Has the meaning in the Scheme Rules
eQR platform	Has the meaning in the Scheme Rules
Electronic Fallback	means Fallback which is electronically generated at a Member's eftpos Terminal, or by the merchant's Acquirer. Applicable to mag stripe cards only.
EMV	means the specifications as published by EMV Co. LLC. Any references to EMV refer to the latest version published, unless otherwise stipulated in these Rules.

Defined Term	eftpos Definition
EMVCo 3-D Secure (3DS)	means the messaging protocol developed by EMVCo to enable consumers to authenticate themselves with their card Issuer.
EMVCo 3DS Specification	means the specifications relating to 3DS as published by EMV Co. LLC from time to time.
EMV Phase 1	means the current transition arrangements through which an eftpos Transaction is created from the use of an EMV compliant Australian IC Card prior to the migration of full EMV functionality for eftpos Transactions.
EMV PTS	means the current version of the specification issued by EMVCo LLC and named EMV Payment Tokenisation Specification.
Encrypted PAN	A surrogate value for a PAN for which there is a direct computational relationship. A cleartext PAN can be derived from the encrypted PAN with access to the appropriate decryption keys.
End Merchant	means an entity which provides goods or services to an eftpos Consumer but does not directly or solely use the services of an eftpos Acquirer, instead receiving services (including settlement) from a Staged Digital Wallet provider or Merchant Service Provider.
Error of Magnitude	means an error (or a series of errors) of or exceeding $2 million or such other amount as may be determined from time to time by the Company.
eTS-F Service Schedule	means the document of that name published by the Company from time to time. Formerly known as eftpos TSP Service Schedule.
Exchange Settlement Account (ESA)	Means an account, maintained with the Reserve Bank of Australia and that is used for the Settlement of eftpos Transactions.

Defined Term	eftpos Definition
Exemption	means approval from the Company in accordance with rule 21 of the Scheme Rules.
Exemption Request	means a request for Exemption submitted by a Member or Direct Connector.
Extreme Risk Merchant category	has the meaning in the Scheme Rules.
Fallback	means a transaction that is used by an Acquirer Member (on behalf of a Merchant) when an eftpos Transaction cannot be completed on-line.
Fixed Frequency Payment	has the meaning in the Scheme Rules.
FTS Event	has the meaning in the Scheme Rules.
FTS Guidelines	means a Guide produced by the Company in relation to failure to settle procedures.
FTS Rules	means the rules set out in section 8 of these Technical, Operational and Security Rules.
Hot Card	means a Card which has been reported by the Cardholder as lost or stolen, or for which there is evidence of fraudulent use.
IAC	has the meaning in the Scheme Rules.
IAC Code Set	has the meaning in the Scheme Rules.
IC Card (or ICC)	means an eftpos Card that contains an integrated circuit and that conforms to the EMV Specifications.

Defined Term	eftpos Definition
Identification and Verification (ID&V)	means the methods used to validate the eftpos Consumer and the eftpos Consumer's Card and eftpos Account at the time of issuance or Provisioning of an eftpos Form Factor.
Indirect Settler	has the meaning in the Scheme Rules.
Insolvency Event	has the meaning in the Scheme Rules.
Instalment Payment	has the meaning in the Scheme Rules.
Interchange	means the exchange of Items for value between eftpos Acquirers and eftpos Issuers or, in the case of Direct Connections with the eftpos Hub, between eftpos Acquirers and the eftpos Hub and the eftpos Hub and eftpos Issuers.
Interchange Fee Report	has the meaning given to it in the document called eftpos Hub Files and Reports
Interchange Line	means the communications channel that provides the medium over which Interchange is supported for a Standard Hub Service.
Interchange Line Encryption	means encryption of the entire message, with the exception of communication headers and trailers that is being passed across an Interchange Line using, as a minimum, double length keys and triple-DES encryption process.
Interchange Link	means each of the logical links between an Acquirer and the eftpos Hub and an Issuer and the eftpos Hub (as the case may be), which facilitates Interchange between them. Interchange Links are supported by an Interchange Line, and are either indirect via a third party intermediary, or direct between an Issuer and the eftpos Hub and an Acquirer and the eftpos Hub.
Interchange Link Message Authentication	means calculation and verification of the Message Authentication Code (MAC) that is being passed across an Interchange Link.

Defined Term	eftpos Definition
Interchange Link PIN Encryption	means encryption of the PIN in accordance with AS2805 Part 3.
Interchange Settlement Report	means a report referred to in clause 8.4.2.
Invalid Transactions	means any of the following: a. Transactions not initiated or authorised by the eftpos Consumer b. Transactions that are not authorised by the Issuer, other than valid Fallback transactions as specified in section 2.12 c. Transactions where the Card or other eftpos form factor is invalid, expired, cancelled or damaged or where the eftpos Consumer's account with its Issuer is closed d. Split transactions occurring in close time proximity to each other when the relevant eftpos Terminalis off-line, which have the effect of avoiding fallback floor limits e. eftpos Consumer is not authenticated by the Issuer for: i. card present contact transactions other than valid Fallback transactions as specified in section 2.12; or ii. card present contactless over the Issuer CVM limit; and f. transactions from another payment system, unless permitted by specific authorisation of the Company g. transactions that the Company has confirmed are a breach or and Technical, Operational and Security Rules; h. transactions using eftpos Digital Acceptance initiated by a Merchant other than an Authorised eftpos Digital Merchant.
Issuer	has the same meaning as eftpos Issuer and Issuer member

Defined Term	eftpos Definition
Issuer Application Data (IAD)	Contains ACe proprietary application data elements to be transmitted to the issuer in an online transaction (in the authorisation request).
Issuer Authentication Data	means the data sent from the issuer to the IC Card for online Issuer Authentication. Contains ARPC.
Issuer Disputed Transaction	means a transaction claimed by the Issuer as being invalid using any of the Chargeback Reason Codes, other than a Consumer Disputed Transaction, whether or not the amount of the transaction has been debited from an eftpos Consumer's account with the Issuer.
Issuer Member	has the meaning in the Scheme Rules.
Issuer Sequence Number	means a one or two digit number used at the option of the Issuer to identify a Card which may have the same primary account number as another Card e.g. primary and secondary cards.
Issuer Wallet	means a mobile wallet hosted by an eftpos Issuer which meets the requirements of these Technical, Operational and Security Rules.
Items	means Credit Items and Debit Items.
Key Encrypting Key (KEK)	means a key which is used to encipher other keys in transport and which can be used to exchange Session Keys between two systems.
Limited Use Credentials (LUC)	means a set of data elements used for generating application cryptograms for either one or a limited number of Transactions
Losses	means all losses, liabilities, damages and claims, and all related costs and expenses (including any and all reasonable legal fees and reasonable costs of investigation, litigation, settlement, judgment, appeal, interest and penalties).

Defined Term	eftpos Definition
Manual Key Entry	means the manual entry of card data including the PAN and the card expiry date.
Marketplace	An entity/intermediary that brings together Cardholders and Merchants on Acceptance Devices, signs up Merchants directly under its own Merchant Identification Number (MID) to accept and process Transactions through a single master account and receives Settlement on behalf of those merchants
Masked PAN	A PAN that has all digits except for at most the first 6 and last 4 replaced with an asterisk or other constant value.
Maximum Single Transaction Amount Limit (MTAL)	The maximum amount of a single transaction that can be accepted by an eftpos ACe enabled card before requiring the transaction to go online. MTAL value is defined by eftpos to enable mandatory offline limits to be utilised.
Medicare Claim Refund	means the payment of a Medicare benefit from Medicare Australia to a patient.
Member	has the meaning in the Scheme Rules.
Member Batch File	means the report referred to in Part 9 of these Technical, Operational and Security Rules.
Merchant	means a person which provides goods or services to an eftpos Consumer and which, in the normal course, is reimbursed by the eftpos Acquirer from the Acceptance Device that it operates, to which it electronically transmits that eftpos Transaction. For the purposes of rule 4.7 of these Technical, Operational and Security Rules, Merchant includes a Stage Digital Wallet Operator, Payment Facilitator and Marketplace.

Defined Term	eftpos Definition
Merchant Category Code (MCC)	means a code assigned to the Merchant that matches the MCCs as outlined in the AS2805.16 for the nature of the business conducted by the Merchant.
Merchant Choice Routing (MCR)	means the mechanism or functionality built in an eftpos Acceptance Device for Merchants to select their preferred application or network for accepting a transaction when presented with two payment applications, rather than by sole reference to the application priority indicator values on a Multi-Network Card. Merchants may express their preference in order to optimise their cost of acceptance.
Merchant Choice Routed transaction	occurs when there are at least two contactless payment applications or networks available that both the Multi-Network Card and Terminal Acceptance Device supported for the transaction, and the Terminal Acceptance Device selected between those applications or networks according to Merchant preference, rather than by sole reference to the application priority indicator values on the card.
Merchant Initiated Transaction	has the meaning in the Scheme Rules.
Merchant Monitoring List	means a list maintained by the Company and made available to Members containing: a. Merchants whose Merchant agreements have been suspended or terminated; and b. Merchants being actively monitored by Acquirers as required by these Technical, Operational and Security Rules.
Merchant Service Provider	means, without limitation, entities that stand between a Merchant and an eftpos Acquirer or Acquirer Member, with or without a Direct Connection and facilitate payments, for example gateways, token requestors, Instalment Payment service provider, third party processors, website service providers, Staged Digital Wallet Operators, aggregators, Payment Facilitators, Marketplaces or

Defined Term	eftpos Definition
	who otherwise provide services to the Merchant for purposes of facilitating eftpos Transactions.
Message Authentication Code	means a code, formed using a secret key, appended to a message to detect whether the message has been altered (data integrity) and to provide data origin authentication. MACs are formed in accordance with AS2805 Part 4.
Mobile Device	includes tablets, phones, watches, wearables and any other device with near field communications capability that meets the minimum operating systems and requirements set out in the eftpos Mobile Member Implementation Guide.
Mobile Wallet	means a mobile wallet hosted by a Mobile Wallet Provider which meets the requirements of these Technical, Operational and Security Rules.
Mobile Wallet Provider	means any of the following CBP Solutions as the context requires: a. provider of an Issuer Wallet; or b. provider of an Open Wallet.
MPoC	means the set of Mobile Payments on COTS requirements adopted and published from time to time by PCI Security Standards Council, LLC.
mPOS	has the meaning in the Scheme Rules
mPOS – EMV TapToMobile	has the meaning in the Scheme Rules
mPOS - SPoC	has the meaning in the Scheme Rules
Multi-Network Card	has the meaning in the Scheme Rules.

Defined Term	eftpos Definition
Node	means a processing centre such as an Acquirer, an Issuer, or an intermediate network facility.
Offline Data Authentication (ODA)	means an asymmetric key pair used for combined dynamic data authentication, the static EMV data associated with the asymmetric key pair.
Off-us Transaction	means an eftpos Transaction that is not an On-us transaction.
One Time Password (OTP)	means a mechanism utilised by the Issuer to perform Cardholder Authentication and confirm that any Token being utilised has not been suspended or deleted or updated. OTP could include SMS message sent to an eftpos Consumer using the details maintained by the Issuer, to advise of a recently received eftpos Digital transaction.
One-time Payment	describes where an eftpos Consumer purchases goods/services online, pays for the goods/services outright at the time of the transaction, and is not committing to making any further payments to the Merchant. "Remember Me" functionality is an extension of One-time payments.
On-Us Transaction	has the meaning in the Scheme Rules.
Open Wallet	means a Mobile Wallet which meets the requirements of these Technical, Operational and Security Rules and is loaded with eftpos Cards and/or eftpos Accounts none or not all of which are issued by the entity providing the Mobile Wallet.
Original Equipment Manufacturer or OEM	means the manufacturer or controller of access to a Mobile Device to which an eftpos Card can be Provisioned to the Secure Element or trusted execution environment, as notified by the Company from time to time. For example and without limitation, a mobile telephone or wearable device manufacturer.

Defined Term	eftpos Definition
OEM Solution	means any: a. embedded Secure Element (eSE) using a certified eftpos applet; or b. a trusted execution environment using approved software, and a Mobile Device, provided by an OEM notified by the Company to Members as being an available eftpos Mobile solution.
PAN	means Primary Account number.
PAR	A non-financial reference assigned to each unique PAN and used to link a Payment Account represented by that PAN to affiliated Payment Tokens.
Participating Member	means a Member participating in a pilot or phase 1 of a rolling launch of any new eftpos product or channel.
Pay As You Go Payment (PAYG)	has the meaning in the Scheme Rules.
Payment Arrangement	has the meaning in the Scheme Rules.
Payment Facilitator	refers to an organisation that provides services to Merchants enabling them to accept card payments. The Payment Facilitator manages the Merchant relationship: it onboards Merchants to its platform, underwrites each merchant, and bills the Merchant for the services necessary to accept card payments.
Payment Token	has the meaning in the EMV Payment Tokenisation Specification, that is a surrogate value for a PAN that is a 13 – 19 digit numeric value that must pass basic validation rules of an account number, including the Luhn check digit. Payment Tokens are generated with a BIN range that has been designated as a Token BIN Range. Payment Tokens must not have the same value as or conflict with a real PAN.

Defined Term	eftpos Definition
PCI DSS	means the Payment Card Industry Data Security Standard adopted and published from time to time by PCI Security Standards Council, LLC.
PCI SSC	means the Payment Card Industry Security Standards Council LLC.
PCI PTS	means the set of PIN Transaction Security requirements adopted and published from time to time by PCI Security Standards Council, LLC.
Permanent Decline	means a decline by an Issuer due to a permanent reason under any of the following codes: 04 - Pick Up Card 14 - Invalid Card Number 36 – Restricted Card 41 - Lost Card 43 - Stolen Card 67 - Hot Card
Physically Secure Device	means a device meeting the requirements specified in ISO 9564-1:2004 for physically secure device.
PIN	has the meaning in the Scheme Rules.
PIN Entry Device (PED)	means a component of a Terminal which provides for the secure entry and encryption of the PIN in processing a Transaction.
PIN Try Counter (PTC)	means an EMV chip card mechanism, which is Issuer-specific for counting the number of unsuccessful consecutive offline PIN tries made by the cardholder. The PIN try counter decrements for each unsuccessful offline PIN verification attempt. When the PTC is zero, the PIN must be blocked and the cardholder cannot be authenticated through the PIN method.

Defined Term	eftpos Definition
PIN Try Limit (PTL)	means an Issuer-specified data element that indicates the maximum number of consecutive incorrect PIN entries. When the cardholder exceeds the PTL the PIN is blocked.
Point of sale (POS)	means the point at which a cardholder makes a payment to a merchant in exchange for goods, services or cash.
Post- Payment Adjustment	has the meaning in the Scheme Rules.
Potential FTS Event	has the meaning in the Scheme Rules.
Prepaid Card	means a card that: a. enables the Prepaid Cardholder to initiate electronic funds transfers at an eftpos Terminal up to a specified amount (subject to any other conditions that may apply to the card); and b. draws on funds held by the Prepaid Program Provider or a third party by arrangement with the Prepaid Program Provider (as opposed to funds held by the Prepaid Cardholder). c. is an eftpos Card that meets the requirements of 3.8 of these Technical, Operational and Security Rules. d. Prepaid Cards may be either non-reloadable/single use or reloadable/multiple use cards.
Prepaid Cardholder	means a person that is in possession of a Prepaid Card.
Prepaid Program Provider	means either: a. an Issuer that issues a Prepaid Card; or b. a person that issues a Prepaid Card in conjunction with a sponsoring Issuer.
Processor	has the meaning in the Scheme Rules.

Defined Term	eftpos Definition
Provisioning	has the meaning in EMV PTS. Clarification - The provisioning process: a. for CBP Solutions includes digitising the eftpos Card or eftpos Account into the Mobile Wallet; and b. for OEM solutions includes delivering the Payment Token and related values, potentially including one or more secret keys for cryptogram generation.
Post-purchase Adjustment	has the meaning in the Scheme Rules.
Purchase	means a transaction that is used by an eftpos Acquirer (on behalf of a Merchant) to obtain authorisation from an eftpos Issuer to complete an eftpos Consumer initiated purchase transaction with a Merchant or service provider.
Quarter	means a 3-month period commencing on 1 January, 1 April, 1 July or 1 October.
RBA	means the Reserve Bank of Australia.
Record of Transaction	has the meaning given in clause 4.11.
Refund	means a transaction that is initiated by an eftpos Acquirer (on behalf of a Merchant) when a Merchant or service provider has a need to return funds to an eftpos Consumer in respect of a prior Purchase; for example, if the eftpos Consumer has returned unwanted goods.
Registered eftpos Consumer	has the meaning in the Scheme Rules.
Re-presentment	means the process by which a Disputed Transaction that has been charged back is re-presented by the Acquirer to the Issuer for payment.

Defined Term	eftpos Definition
Restoration Period	has the meaning in the Standard Hub Service Schedule.
Recurring Payment	has the meaning in the Scheme Rules.
Risk Based Analysis	has the meaning in the Scheme Rules.
RITS	has the meaning in the Scheme Rules.
RITS Batch Feeder	means the technical interface to RITS.
RITS Instruction	has the meaning in the Scheme Rules.
RITS Recall Instruction	means a file in the format prescribed by the Reserve Bank of Australia and complying with the specifications for the RITS Batch Feeder for the recall of a Batch Instruction.
RITS Business Day	has the meaning in the Scheme Rules.
Secure Cryptographic Device (SCD)	means a physically and logically protected hardware device that provides a set of secure cryptographic services. PIN Entry Devices and Security Control Modules are two specific instances of Secure Cryptographic Devices.
SCD Security Standards	means the standards from time to time published by the Australian Payments Network in relation to SCD's.
Scheme Fee	means all the fee owed by the Member to the Company at any time, including but not limited to the scheme fee, Infrastructure fee, ATM processing fee, Dispute & Arbitration fee.
Scheme Fee Report	has the meaning given to it in the document called eftpos Hub Files and Reports.

Defined Term	eftpos Definition
Scheme Rules	means the rules adopted by the Company in accordance with the Constitution.
Secure Element or ESE	means a tamper-resistant chip embedded in a Mobile Device for the purposes of hosting applications securely to protect access to the application and the data stored within each application, including confidential and cryptographic data. For the purposes of eftpos Mobile, eftpos will notify Members of any OEM that has embedded an eftpos applet into a Secure Element.
Security Control Module (SCM)	means a physically and logically protected hardware device that provides a set of secure cryptographic services.
Security Policy	means the policy adopted by the Company from time to time and communicated to Members for the secure exchange of information between Members and the Company.
Service Provider	has the meaning in the Scheme Rules.
Session Key	is a generic reference to any one of a group of keys used to protect transaction level data. Session keys exist between two discrete points within a network e.g. host-to-host and host-to-Terminal.
Settlement	has the meaning in the Scheme Rules.
Settlement Agent	has the meaning in the Scheme Rules.
Settlement Cut-over Time	means on each day, the latest time for Transactions processed that are taken to have occurred on that day. Transactions processed after such time are taken to have occurred on the next day.

Defined Term	eftpos Definition
SFTP	means the secure file transfer protocol adopted by the Company from time to time and communicated to Members.
Single Payment	has the meaning in the Scheme Rules.
SPoC	means the set of Software-based PIN entry on COTS requirements adopted and published from time to time by PCI Security Standards Council, LLC
Staged Digital Wallet	means a Digital Wallet that is not a Mobile Wallet and is: a. usable at more than 1 retailer b. used for payment from eftpos Consumer to End Merchant that occurs in two distinct stages which can occur in any order: i. **Payment Stage** – the Staged Digital Wallet operator pays the End Merchant ii. **Funding Stage** - a transaction is initiated on the stored card details, through which the Staged Digital Wallet Operator receives funds c. The End Merchant never receives card details
Staged Digital Wallet Operator	means an Australian entity that owns and operates the Staged Digital Wallet.
Standard Hub Direct Connection	has the meaning in the Scheme Rules.
Standard Hub Service	has the meaning in the Scheme Rules.
Standard Hub Service Schedule (SHSS)	means the document of that name published by the Company from time to time.

Defined Term	eftpos Definition
Statistically Unique	means an acceptably low statistical probability of an entity (e.g. a key) being duplicated by either chance or intent.
Strong Customer Authentication	means a method of authenticating a Cardholder with two authentication methods instead of one, being a combination of something the customer knows (for example a PIN or passcode or OTP), something the customer has (for example a device or Token) and/or something the customer is (for example biometrics), including without limitation 3DSecure 2.x. and eftpos Secure.
Survivor	means, in relation to an FTS Event, each Member other than the DSEP.
Tamper Responsive SCM	means a Security Control Module that when operated in its intended manner and environment, will cause the immediate and automatic erasure of all keys and other secret data and all useful residues of such data when subject to any feasible attack. A Tamper Responsive SCM must comply with the requirements of Section 5.
Terminal	means an eftpos Terminal. See also “Chip capable Terminal” “Contactless capable Terminal” “Chip enabled Terminal”.
Terminal Application Validation (TAV)	Test methodology used by the eftpos Certification Body for contact Terminalchip applications**.**
Terminal Identification Number	means the unique number assigned by an Acquirer to identify a particular Terminal.
Terminal Sequence Number	means a number allocated sequentially to each Transaction by the relevant Terminal.

Defined Term	eftpos Definition
Technology Fallback	means a transaction processed online using the magnetic stripe when an eftpos Terminal is unable to communicate with a card's Chip.
Token	means a Payment Token or an Acquiring Token as the case requires and as permitted by the Company from time to time.
Token BIN	means a specific BIN that has been designated only for the purpose of issuing Payment Tokens and is flagged accordingly in BIN Database.
Token Cryptogram	has the meaning in EMV PTS
Token Domain	has the meaning in EMV PTS.
Token Domain Restriction Controls	in accordance with the EMV Payment Tokenisation Specification, means a set of parameters established as part of Payment Token issuance by the Token Service Provider that will allow for enforcing appropriate usage of the Payment Token in Transactions. Examples of the controls include, each in accordance with these Technical, Operational and Security Rules: a. use of the Payment Token with particular presentment modes, such as contactless or e-commerce b. use of the Payment Token at a particular Merchant that can be uniquely identified c. verification of the presence of a Token Cryptogram that is unique to each Transaction.
Token Issuance	means: a. for Payment Tokens - the process where a Payment Token is created and delivered to a Token Requestor in accordance with the EMV Payment Tokenisation Specification; or

Defined Term	eftpos Definition
	b. for Acquiring Tokens - the process where an identifier in replacement for a PAN is created and delivered to a Token Requestor.
Token Requestor	means an eftpos Member, an OEM or a Direct Connector acting on behalf of an eftpos Member that is seeking to implement or manage Tokenisation according to the eftpos Technical, Operational and Security Rules. The Token Requestor is responsible for initiating requests for PANs to be Tokenised by submitting Token Requests to the Token Service Provider. Where the Company is the TSP, the Token Requestors include: a. any OEM notified by the Company from time to time; b. eftpos Issuers; c. eftpos Acquirers; d. Merchants or Merchant Service Providers notified by the Company from time to time; or e. a Direct Connector acting on behalf of an eftpos Member.
Token Service Provider (TSP)	means an entity that issues a Payment Token or Acquiring Token (as the case may be) in respect of an eftpos Form Factor.
Tokenisation	when applied to data security, means the process of substituting a sensitive data element with a non-sensitive equivalent, referred to as a token, which has no extrinsic or exploitable meaning or value.
Transaction	means an eftpos Transaction.
Transaction Settlement Date	means the date that the eftpos Hub assigns to the eftpos Transaction, derived from field 15 of an eftpos Transaction message – there is only one Transaction Settlement Date per calendar day.

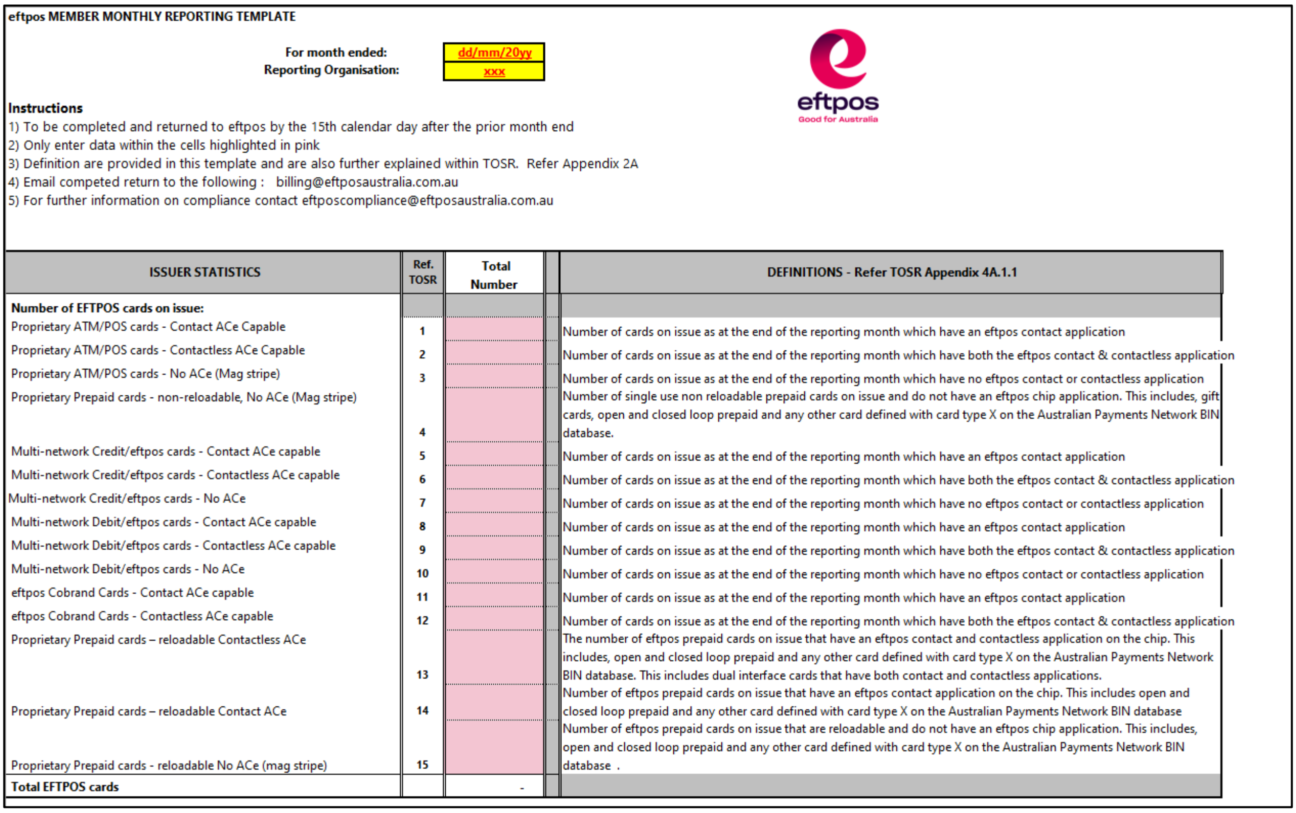
Defined Term	eftpos Definition
Track Two Equivalent Data	means the contents of the EMV data element tag 57. This data element contains the data elements of track two according to ISO/IEC 7813, excluding start sentinel, end sentinel and Longitudinal Redundancy Check.
Transaction Authentication	means the process of validating that the individual initiating an eftpos Digital transaction on a payment card is the rightful owner of those card details. There are two methods of Transaction Authentication – Transaction Authentication by Issuer, and Transaction Authentication by Merchant.
Transaction Authentication by Issuer	means at the time of the transaction or, in the case of Fixed Frequency, Pay As You Go or Instalment Payments, at the time of the first transaction in the series for the purposes of any payment system, the Issuer directly validates that the transaction has been initiated by the authorised cardholder (e.g. via a OTP or 2FA mechanism utilised by the Issuer or, from the date specified by the Company, by eftpos Secure.
Transaction Authentication by Merchant	means at the time of the transaction or, in the case of Fixed Frequency, Pay As You Go or Instalment Payments, at the time of the first transaction in the series for the purposes of any payment system, the Merchant must be able to validate that the individual initiating the transaction is the same individual who was previously authenticated by an Issuer for the purposes of any payment system as the rightful owner of a card through a Cardholder Authentication step. This does not necessarily involve explicitly requiring the customer to re-enter their credentials at transaction time. E.g. the merchant may require the customer to log into the wallet using their credentials before performing transactions and allow that log-in to remain valid for a particular period of time, from a particular device, or until the customer chooses to log-out.
Transit Scheme	means a transport system managed by a Transit Scheme Operator, for the purpose of providing transport services to consumers.

Defined Term	eftpos Definition
Transit Scheme Operator	means a Merchant who operates a Transit Scheme. A Transit Scheme Operator may provide transport services directly to consumers or through a Transit Service Provider.
Transit Service Provider	means an entity who subscribes to a Transit Scheme that provides services to a Transit Scheme Operator or consumers as intermediary between the Transit Scheme Operator and consumers in accordance with the terms of that Transit Scheme.
Triple-DES (3DES)	means the encryption and decryption of data using a defined compound operation for the DEA-1 encryption and decryption operations. Triple-DES is described in AS2805 Part 5.4.
Trusted Service Manager (TSM)	means the entity that managed the Payment Token lifecycle events which for OEM Solutions is the Company and for CBP Solutions may be the Company.
Upper Consecutive Offline Transaction Limit (UCOL)	A field which denotes the maximum number of consecutive Chip fallback transactions that can be accepted by the card before requiring the transaction to go online. The lowest value that an Issuer can use in this field is specified by the Company.
Upper Cumulative Offline Transaction Limit (UCOTA)	A field which denotes the maximum cumulative Chip fallback amount that can be accepted by the card before requiring the transaction to go online. The lowest value that an Issuer can use in this field is specified by the Company.

Appendix B. Reporting to the Company

B.1 Member Monthly Reporting format

A soft copy template of the Member Monthly Report can be accessed via the eftpos secure portal and the Member section of the resources page of the eftpos Australia website.



eftpos MEMBER MONTHLY REPORTING TEMPLATE

For month ended: dd/mm/20yy
Reporting Organisation: xxx

Instructions

1) To be completed and returned to eftpos by the 15th calendar day after the prior month end
2) Only enter data within the cells highlighted in pink
3) Definition are provided in this template and are also further explained within TOSR. Refer Appendix 2A
4) Email competed return to the following : billing@eftposaustralia.com.au
5) For further information on compliance contact eftposcompliance@eftposaustralia.com.au

ISSUER STATISTICS	Ref. TOSR	Total Number	DEFINITIONS - Refer TOSR Appendix 4A.1.1
Number of EFTPOS cards on issue:			
Proprietary ATM/POS cards - Contact ACe Capable	1		Number of cards on issue as at the end of the reporting month which have an eftpos contact application
Proprietary ATM/POS cards - Contactless ACe Capable	2		Number of cards on issue as at the end of the reporting month which have both the eftpos contact & contactless application
Proprietary ATM/POS cards - No ACe (Mag stripe)	3		Number of cards on issue as at the end of the reporting month which have no eftpos contact or contactless application
Proprietary Prepaid cards - non-reloadable, No ACe (Mag stripe)	4		Number of single use non reloadable prepaid cards on issue and do not have an eftpos chip application. This includes, gift cards, open and closed loop prepaid and any other card defined with card type X on the Australian Payments Network BIN database.
Multi-network Credit/eftpos cards - Contact ACe capable	5		Number of cards on issue as at the end of the reporting month which have an eftpos contact application
Multi-network Credit/eftpos cards - Contactless ACe capable	6		Number of cards on issue as at the end of the reporting month which have both the eftpos contact & contactless application
Multi-network Credit/eftpos cards - No ACe	7		Number of cards on issue as at the end of the reporting month which have no eftpos contact or contactless application
Multi-network Debit/eftpos cards - Contact ACe capable	8		Number of cards on issue as at the end of the reporting month which have an eftpos contact application
Multi-network Debit/eftpos cards - Contactless ACe capable	9		Number of cards on issue as at the end of the reporting month which have both the eftpos contact & contactless application
Multi-network Debit/eftpos cards - No ACe	10		Number of cards on issue as at the end of the reporting month which have no eftpos contact or contactless application
eftpos Cobrand Cards - Contact ACe capable	11		Number of cards on issue as at the end of the reporting month which have an eftpos contact application
eftpos Cobrand Cards - Contactless ACe capable	12		Number of cards on issue as at the end of the reporting month which have both the eftpos contact & contactless application
Proprietary Prepaid cards – reloadable Contactless ACe	13		The number of eftpos prepaid cards on issue that have an eftpos contact and contactless application on the chip. This includes, open and closed loop prepaid and any other card defined with card type X on the Australian Payments Network BIN database. This includes dual interface cards that have both contact and contactless applications.
Proprietary Prepaid cards – reloadable Contact ACe	14		Number of eftpos prepaid cards on issue that have an eftpos contact application on the chip. This includes open and closed loop prepaid and any other card defined with card type X on the Australian Payments Network BIN database
Proprietary Prepaid cards - reloadable No ACe (mag stripe)	15		Number of eftpos prepaid cards on issue that are reloadable and do not have an eftpos chip application. This includes, open and closed loop prepaid and any other card defined with card type X on the Australian Payments Network BIN database .
Total EFTPOS cards		-	

B.2 Issuing

B.2.1. Card issuing

1. Proprietary eftpos cards - Contact ACe capable - The number of eftpos only cards on issue that have an eftpos contact application on the cards chip. This excludes dual interface cards that have both contact and contactless applications.
2. Proprietary eftpos cards – Contactless ACe capable – The number of eftpos only cards on issue that have an eftpos contactless application on the cards chip. This includes dual interface cards that have both contact and contactless applications.
3. Proprietary eftpos cards, no ACe (Mag stripe) - The number of eftpos only cards on issue that do not have an eftpos chip or contactless application.
4. Proprietary Prepaid cards - non-reloadable, no ACe (Mag stripe) - The number of non-reloadable/single use eftpos prepaid cards on issue that do not have an eftpos chip application. This includes, gift cards, open and closed loop prepaid and any other card defined with card type X on the Australian Payments Network BIN database.
5. Multi-Network Credit/eftpos cards - Contact ACe capable – The number of Multi-Network credit cards (a Multi-Network credit card can be used to initiate either an eftpos transaction or a transaction that is processed by another payment system accessing a credit account and/or a combined deposit and credit account) on issue that have an eftpos contact application on the cards chip. This excludes dual interface cards that have both contact and contactless applications.
6. Multi-Network Credit/eftpos cards - Contactless ACe capable -The number of Multi-Network credit cards on issue that have an eftpos contactless application on the cards chip. This includes dual interface cards that have both contact and contactless applications.
7. Multi-Network Credit/eftpos cards - No ACe - The number of Multi-Network credit cards on issue that do not have an eftpos contact or contactless application on the cards chip.
8. Multi-Network Debit/eftpos cards - Contact ACe capable - The number of Multi-Network debit cards (a Multi-Network debit card can be used to initiate either an eftpos transaction or a transaction that is processed by another payment system accessing a deposit account) on issue that have an eftpos contact application on the cards chip. This excludes dual interface cards that have both contact and contactless applications.
9. Multi-Network Debit/eftpos cards - Contactless ACe capable - The number of Multi-Network debit cards on issue that have an eftpos contactless application on the cards chip. This includes dual interface cards that have both contact and contactless applications.
10. Multi-Network Debit/eftpos cards - No ACe- The number of Multi-Network debit cards on issue that do not have an eftpos contact or contactless application on the cards chip.

11. eftpos Cobrand Cards - Contact ACe capable - The number of eftpos Cobrand Cards (a eftpos Cobrand Card can be used to initiate either an eftpos transaction or a transaction that is processed by another payment system accessing a deposit account) on issue that have an eftpos contact application on the cards chip. This excludes dual interface cards that have both contact and contactless applications.
12. eftpos Cobrand Cards - Contactless ACe capable - The number of eftpos Cobrand Cards on issue that have an eftpos contactless application on the cards chip. This includes dual interface cards that have both contact and contactless applications.
13. Proprietary Prepaid cards – reloadable Contactless ACe - The number of eftpos prepaid cards on issue that have an eftpos contact and contactless application on the chip. This includes open and closed loop prepaid and any other card defined with card type X on the Australian Payments Network BIN database. This includes dual interface cards that have both contact and contactless applications.
14. Proprietary Prepaid cards – reloadable Contact ACe - The number of eftpos prepaid cards on issue that have an eftpos contact application on the chip. This includes open and closed loop prepaid and any other card defined with card type X on the Australian Payments Network BIN database.
15. Proprietary Prepaid cards - reloadable no ACe (mag stripe) - The number of reloadable eftpos prepaid cards on issue that do not have an eftpos chip application. This includes open and closed loop prepaid and any other card defined with card type X on the Australian Payments Network BIN database.

B.3 Acquiring

Some Acquirers also act as a switch for other Members or aggregators. Members who acquire transactions for third parties or who have third parties acquire transactions on their behalf, may report their own Acquiring activity and the Acquiring activity performed by or for third parties separately. Acquiring Members must report their own Acquiring activity in the section entitled Acquirer Statistics - Own. Acquirers that wish to report third party activity separately should use the section entitled Acquirer Statistics - Other. When optionally reporting third party activity separately, Members must not include the third party figures in both sections.

B.3.1. POS acceptance

1. Merchants - The total number of individual merchants that accept eftpos Transactions.
2. Merchant locations - The total number of merchant locations (e.g. number of store locations) that only accept eftpos Transactions

3. Terminals - Contact ACe capable - The total number of Terminals that are capable of processing eftpos Transactions from a card using the cards eftpos contact application. This excludes Terminals that are dual interface, i.e. they are capable of processing transactions from a card using either the cards eftpos contact or contactless application.
4. Terminals - Contactless ACe capable - The total number of Terminals that are capable of processing transactions from a card using the cards eftpos contactless application. This includes Terminals that are dual interface, i.e. they are capable of processing transactions from a card using either the cards eftpos contact or contactless application.
5. Terminals - Not ACe capable - The total number of Terminals that only process purchase transactions that are incapable of processing transactions using a cards eftpos contact or contactless application.

Appendix C. Electronic File Transfer Protocol

Members are to arrange a Secure File Transfer Protocol (SFTP) with the Company to enable secure production batch file uploads, for reporting purposes. This appendix provides the process and information to establish an SFTP connection with the Company.

This appendix explains the high level process and requirements, for other more technical information, please contact eftpos technical staff (Refer to D1.1).

C.1 FTP

C.1.1. Agree IP Address and port numbers for Secure FTP servers

The Company has a primary and a secondary SFTP server available for file transfer. The primary server is the active server where a Member's production batch files are received. The secondary server is redundancy back-up only.

The Company will provide Members with IP addresses and port numbers for test and production batch file destinations upon receipt of an 'eftpos Secure FTP application form'. Refer to D1.1.

C.1.2. Set up login credentials

SFTP (SSH 1) to the Company requires the Company and the Member to set up a password and a certificate. The Member needs to provide a public key, user name and password to the Company pre-installed into the Company's SFTP server for authentication when the file is sent to the Company.

The Company can generate a public/private key for Members. Please contact eftpos technical staff (refer D1.1).

C.1.3. Schedule Batch File delivery

The Member must inform the Company of the days and time the Member will provide the production batch file to the Company. The Company will schedule the application to poll and process the production batch file after the stated time.

Members must provide production batch files on a daily basis. The Company and the Member may arrange to receive the files more than once a day.

Members should send production batch files prior to or at the agreed and scheduled time to ensure it is processed without delay. If the Company does not receive a production batch file as scheduled, the Company will inform the Member that the file was not received as scheduled. In accordance with the eftpos Hub Files and Reports – POS Specification, two transfer mechanisms must be supported. In the event of a primary transmission failure, Members will revert to the secondary method if they cannot resolve the primary method within 48 hours of a failed file.

Members must inform the Company in at least 5 working days prior whether the Member intends to provide a production batch file in the event of any public holiday, including state-wide, nationwide and bank holidays.

C.1.4. Set up acknowledgement file delivery

The Member must inform the Company of the nominated email address. The Company will respond to each production batch file by way of an automatic acknowledgement file sent to the Member's nominated email address. If the Company does not receive a production batch file at the scheduled time or a file is corrupted, the Company will investigate the problem and advise the Member to resend the file. Members will revert to the secondary method if they cannot resolve the primary method within 48 hours of a failed file.

System test plan

Prior to file transfer, the Member and the Company will validate the procedure and configuration using the following steps:

C.1.4.1 Test set up

1. The Member and the Company will agree a system test window, walk through the test plan and agree the system test success criteria.
2. The Company will provide an IP address and port number to the Member to configure a SFTP session.
3. The Member will generate public and private keys and will install their private key in their own server and forward the public key to the Company for the Company to install in their primary and secondary servers.
4. The Member will provide a user name and a password to the Company to enable the member to log on to the Company SFTP server.
5. The Company will install the Member's user name and password on the eftpos primary and secondary servers.

6. Test the file transfer process
7. The Member will create at least two large files of any format of at least 10Mb each. These files do not need to contain sample Transaction data. The files must use the correct file naming convention, as set out in the eftpos Hub Files and Reports – POS Specification.
8. The Member will establish a connection to the Company using the IP address and port provided in step 2, then upload the sample files created in step 6 to test the transfer process.
9. The Company will respond to this test to confirm success or otherwise.
10. Test batched transaction processing
11. The Member will create a test batch file containing sample transactions in the format specified in the eftpos Hub Files and Reports – POS Specification.
12. The Member will notify the Company of the timing of the delivery of the test batch file to the Company.
13. At the notified time, the Member will establish a connection to the Company using the IP address and port provided in step 2, to test connectivity.
14. The Member will upload one test batch file to the Company server.
15. On the following day the Company will respond by way of an Acknowledgement File to confirm the test batch file was successfully processed.
16. The Member will confirm receipt of the acknowledgement file verbally.
17. The Member will review the data via the Company's portal (Members must request access to the portal prior to initiating a system test. The Company will provide the member with a username and password) to verify the Company has received and processed the data correctly.
18. Test closure.
19. The Member and the Company will agree the success criteria of the test are met or will work together to rectify any issues with the secure file transfer process and batch file processing.

Appendix D. eftpos Secure FTP application form

D.1 eftpos SFTP application form

Members are required to complete and submit the application form below:

eftpos Secure File Transfer Application Form	
Full Name:	
Organisation:	
Address:	
Job Title:	
Telephone:	
Mobile Phone:	
Email address:	
Preferred user name:	
Password:	eftpos will communicate passwords via telephone.
Scheduled delivery frequency:	For example: Business days only or Weekdays.
Scheduled delivery time:	For example: Midnight
Email address for Acknowledgement files	
Do you require eftpos to produce public private keys?	Yes / No
Will the file be encrypted before the transfer?	Yes / No
If files are to be encrypted, please indicate the method of encryption	
Signature: ______________________ Name: ______________________	Date:
eftpos use	
IP Address:	
Port No:	

D.1.1. eftpos Technical staff contacts

Below are the eftpos contacts for support if any technical problems require attention:

eftpos	Contact Name	Contact Number	Email Address
Business hours:	Senior Systems Analyst	02 8270 1800	support@eftpospayments.com.au
After hours:	Senior Systems Analyst	TBA	support@eftpospayments.com.au

Confidential. Member use only

Appendix E. Reference documents

E.1 Reference documents

Document Number	Document Name
AS2805.2:2015	Electronic Funds Transfer - Requirements for interfaces Part 2: Message structure, format and content
AS2805.4.1-2001/Amdt 1/2006	Electronic Funds Transfer – Requirements for interfaces Part 4: Message authentication – Mechanism using a blockcipher
AS2805.6.3-2000/Amdt 1/2003	Electronic Funds Transfer – Requirements for interfaces Part 6.3: Key management – Session Keys – Node to node
AS2805.6.1-2000/Amdt 1/2003	Electronic Funds Transfer – Requirements for interfaces Part 6.3: Key management – Principles
AS2805.6.6-2006	Electronic Funds Transfer – Requirements for interfaces Part 6.6: Key management – Session keys – Node to node with KEK replacement
AS2805.9-2000	Electronic Funds Transfer – Requirements for interfaces Part 9: Privacy of communications
AS2805.12.2-1999	Electronic Funds Transfer – Requirements for interfaces Part 12.2: Message content - Codes
PCI DSS	Payment Card Industry Data Security Standard – Version 4.0

E.2 eftpos Reference documents

Document name	Document purpose
eftpos Scheme Rules	Rules governing all participants of the eftpos Payment System.
eftpos Standard Hub Service Schedule	Sets out requirements and agreements relating to the eftpos Hub.
eftpos Hub Link Specification	Technical specification for interchange communications between eftpos Hub and Direct Connectors.
eftpos Hub Files and Reports Specification - POS	Technical specification for report and files sent and received as part of a Direct Connection to the eftpos Hub.
eftpos Card Application Personalisation Specification.	Technical specification for the personalisation of eftpos Cards.
eftpos Brand and Style Guide	Sets out branding requirements and approval process for the use of the eftpos Brand Mark across eftpos Products and Channels.
eTS-F Service Schedule	Defines the operating principles and agreed terms and conditions for use of, and onboarding to, the eTS-F product.
eftpos Secure Service Schedule	Defines the operating principles and agreed terms and conditions for use of, and onboarding to, the eftpos Secure product.
eQR Service Schedule	Defines the operating principles and agreed terms and conditions for use of, and onboarding to eQR.
eftpos API Service Schedule	Defines the operating principles and agreed terms and conditions for use of, the eftpos API service
eftpos Mobile Service Schedule	Defines the operating principles and agreed terms and conditions for use of, and onboarding to, the eftpos Mobile product