

Effective:  
1 January 2020  
Version 010

# **AUSTRALIAN PAYMENTS NETWORK LIMITED**

ABN 12 055 136 519

**A Company limited by Guarantee**

## **Code Set**

for

## **ISSUERS AND ACQUIRERS COMMUNITY FRAMEWORK**

### **Volume 7 Card Not Present Code**

Commenced 1 July 2019

Copyright © 2019 - 2020 Australian Payments Network Limited  
ABN 12 055 136 519

#### **Australian Payments Network Limited**

Level 23, Tower 3, International Towers Sydney, 300 Barangaroo Avenue, SYDNEY NSW 2000  
Telephone: (02) 9216 4888

**Code Set for**  
**ISSUERS AND ACQUIRERS COMMUNITY**  
**FRAMEWORK**

**Volume 7**  
**Card Not Present Code**

**INDEX**

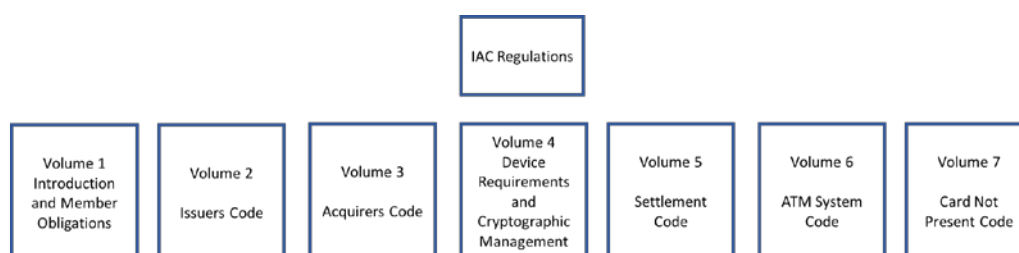
<b>PART 1</b>	<b>PURPOSE, APPLICATION AND DEFINITIONS .....</b>	<b>1.1</b>
1.1	Purpose of this Code.....	1.1
1.2	Application.....	1.1
1.3	Out of Scope .....	1.2
1.4	Definitions .....	1.2
<b>PART 2</b>	<b>ANALYSIS AND AUTHENTICATION.....</b>	<b>2.1</b>
2.1	Analysis and Authentication Types.....	2.1
2.1.1	Risk Based Analysis .....	2.1
2.1.2	Strong Customer Authentication (“SCA”) .....	2.1
2.2	Exempt Transactions.....	2.1
2.2.1	Recurring Transaction .....	2.2
2.2.2	Trusted Customer Transaction.....	2.2
2.2.3	Wallet Transactions .....	2.3
<b>PART 3</b>	<b>IAC PARTICIPANT OBLIGATIONS .....</b>	<b>3.1</b>
3.1	Obligations on Issuers.....	3.1
3.1.1	Issuer Fraud Rate and Threshold .....	3.1
3.1.2	Issuer Compliance .....	3.2
3.1.3	Issuer Reporting .....	3.2
3.2	Obligations on Acquirers .....	3.3
3.2.1	Merchant Fraud Rate and Threshold .....	3.4
3.2.2	Acquirer Compliance .....	3.5
3.2.3	Acquirer Reporting.....	3.5
<b>PART 4</b>	<b>THRESHOLD REQUIREMENTS AND SANCTIONS.....</b>	<b>4.1</b>
<b>PART 5</b>	<b>APPENDICES .....</b>	<b>5.1</b>
5.1	Issuer Report Template.....	5.1
5.2	Merchant Breach Report Template.....	5.3
5.3	Acquirer Trend Report Template .....	5.4

## PART 1 PURPOSE, APPLICATION AND DEFINITIONS

### 1.1 Purpose of this Code

The IAC has been established to develop, implement and operate effective standards, policies and procedures to promote the efficiency, security and integrity of Australian Card Payments. These include minimum security standards, interoperability standards and value added services that support how payment cards are used throughout Australia.

These standards and requirements are contained within the IAC Code Set which is structured as follows:



The Card Not Present Fraud Mitigation Framework (**CNP Framework**) was created in 2019 in consultation with relevant stakeholders in the payments industry. The CNP Framework sets out an approach to mitigating the impact of card-not-present payments fraud for merchants, consumers, Issuers, Acquirers, card schemes, payment gateways, payment system providers, and regulators. It is designed to reduce fraud in CNP online channels, while ensuring that online transactions continue to grow.

Volume 7 implements the CNP Framework into the IAC Code Set. Volume 7 contains additional mandatory obligations for Issuers and Acquirers to those found in Volumes 2 and 3 of the IAC Code Set.

### 1.2 Application

This Volume 7 applies to Australian acquired CNP Transactions conducted using Australian issued cards which are not Out of Scope Transactions.

Volume 7 codifies and gives effect to the matters the subject of the CNP Framework and as such operates to the exclusion of, and take precedence over, the CNP Framework.

Notes in this Volume 7 are included for guidance only and are not operative provisions of the IAC Code Set.

### 1.3 Out of Scope

This Volume 7 does NOT apply to the following:

- (a) CNP Transactions conducted by MOTO (except where expressly referred to in the reporting obligations at clause 3.3 and 3.5.1) and manual entry; and
- (b) CNP Transactions in which the card used is a corporate card, gift card or pre-paid card.

Amended  
effective 1.1.20

*Note: The following, by definition and application of this Code in clause 1.2 are also Out of Scope Transactions:*

Amended  
effective 1.1.20

- (a) *transactions in which the cardholder is physically present, including POS payments and ATM withdrawals or transfers.*
- (b) *non-card remote commerce transactions; and*
- (c) *CNP transactions acquired outside of Australia, and cards issued outside of Australia.*

*Future iterations of this Volume may consider transaction types currently deemed out of scope. In the meantime, however, IAC Participants are strongly encouraged to take a “best effort” approach to apply SCA principles and mitigate fraud for transactions acquired outside of Australia.*

### 1.4 Definitions

In this IAC Code Set the following words have the following meanings unless the contrary intention appears.

“**Acquirer**” is defined in the IAC Regulations and means a Constitutional Corporation that in connection with a Transaction:

Amended  
effective 1.1.20

- (a) under arrangement with and on behalf of an Issuer, discharges the obligations owed by that Issuer to the relevant Cardholder; and
- (b) engages in Interchange Activity with that Issuer as a result.

“**Acquirer Identification Number**” and “**AIN**” The six-digit number assigned by ISO to identify an acquiring Framework Participant (see also IIN, BIN).

“**Acquirer Reference Number**” [Deleted]

Deleted  
effective 20.8.18

“**AID**” means Application ID present in an ICC chip card.

Inserted  
effective  
21.11.17

**“Approved Cardholder”** means:

Inserted  
effective 1.1.16

- (a) a customer of an Issuer (or third party represented by an IA Participant) who has been issued with a Card and a PIN by that IA Participant or by a third party represented by the IA Participant; or
- (b) any person who operates an account or has access to an account held with an IA Participant (or third party represented by an IA Participant) who has been issued with a Card and PIN by the IA Participant (or third party represented by an IA Participant).

**“Approved Card Payment System”** is defined in the IAC Regulations and means a Card Payment System which:

Amended  
effective 1.1.20

- (a) is, or is eligible to be, a Recognised APS; and
- (b) is determined by the IAF to satisfy the Approval Criteria for Approved Card Payment Systems.

**“Approved Device”** means a Secure Cryptographic Device that has been evaluated in accordance with clause 3.1 of the IAC Code Set Volume 4 (Device Requirements and Cryptographic Management) which has been approved for use within IAC.

Amended  
effective 1.1.16

**“Approved Evaluation Facility”** and **“AEF”** means a testing laboratory that has been accredited by the Company to conduct SCD security compliance testing and is listed on the Company’s website as an Approved Evaluation Facility.

Amended  
effective 1.1.19

**“Approved Non-standard POI Technology”** means a Non-standard POI Technology that has been evaluated in accordance with Annexure G of the IAC Code Set Volume 4 (Device Requirements and Cryptographic Management) and approved for use within IAC.

Inserted effective  
1.1.20

**“Approved SPoC Solution”** means a SPoC solution that has been evaluated in accordance with Annexure G of the IAC Code Set Volume 4 (Device Requirements and Cryptographic Management) and approved for use within IAC. All such SPoC solutions must have been approved by PCISSC prior to evaluation by AusPayNet.

Inserted effective  
1.1.19

**“AS”** means Australian Standard as published by Standards Australia.

**“ATM”** or **“ATM Terminal”** means an approved electronic device capable of automatically dispensing Cash in response to a Cash withdrawal Transaction initiated by a Cardholder. Other Transactions (initiated by a Card) such as funds transfers, deposits and balance enquiries may also be supported. The device must accept either magnetic stripe Cards or smart (chip) Cards where Transactions are initiated by the Cardholder keying in a Personal Identification Number (PIN). Limited service devices (known as “Cash dispensers”) that only allow for Cash withdrawal are included.

Amended  
effective 1.1.16

- “ATM Access Regime”** means the access regime imposed by the Reserve Bank of Australia under section 12 of the *Payment Systems (Regulation) Act 1998* by regulatory instrument dated 23 February 2009. Inserted effective 1.1.16
- “ATM Affiliate”** means an Affiliate which has subscribed to IAC Code Set Volume 6 (ATM System Code). Last amended effective 1.1.20
- “ATM Code Committee”** means the committee established by the IAF pursuant to Part 11 of the IAC Regulations. Inserted effective 1.1.16
- “ATM Direct Charging Date”** means 3 March 2009.
- “ATM Framework Participant”** means a Constitutional Corporation which pursuant to the IAC Regulations, is a Framework Participant in the IAC, and is a subscriber to IAC Code Set Volume 6 (ATM System Code) pursuant to Part 2, clause 2.2 of Volume 6 and includes, for the avoidance of doubt, each: Last amended effective 1.1.20
- (a) IA Participant;
  - (b) ATM Operator Member; and
  - (c) ATM Affiliate.
- “ATM Interchange”** is defined in the IAC Regulations and means the exchange of payment instructions for value between Acquirers (whether for itself or on behalf of a third party) and Issuers, via an Interchange Link, as a result of the use of an Issuer’s Card by a Cardholder to generate an ATM Transaction. Interchange arrangements may, but need not, be reciprocal. Last amended effective 1.1.20
- “ATM Law”** means a law of the Commonwealth or of any State or Territory in relation to the operation of ATM Terminals. Inserted effective 1.1.16
- “ATM Operator Fee”** means a fee paid by a Cardholder to the operator of an ATM to effect a Transaction through their Terminal.
- “ATM Operator Member”** means an Operator Member which has subscribed to IAC Code Set Volume 6 (ATM System Code). Last amended effective 1.1.20
- “ATM System”** is defined in the IAC Regulations and means the network of direct and indirect Interchange Lines, Interchange Links, associated hardware, software and operational procedures that facilitate the transmission, authorisation and reconciliation of ATM Transactions between IA Participants in Australia. Amended effective 1.1.20
- “ATM Transaction”** is defined in the IAC Regulations and means, for the purposes of this IAC Code Set, a Cash deposit, a Cash withdrawal, or a balance enquiry effected by a Cardholder at an ATM. Amended effective 1.1.20
- “ATM Transaction Listing”** means a listing which complies with the requirements of Part 4, clause 11 of the IAC Code Set Volume 6 (ATM System Code). Amended effective 1.1.16

“**AusPayNet**” is defined in the IAC Regulations and means Australian Payments Network Limited (ABN 12 055 136 519).

Amended  
effective 1.1.20

“**Australian IC Card**” means an IC Card in respect of which the EMV Issuer Country Code data element (tag 5F28) equal to “036” (Australia).

“**Authentication**” [Deleted]

Deleted  
effective 1.1.20

“**Authorisation**” in relation to a Transaction, means confirmation given by an Issuer that funds will be made available for the benefit of an Acquirer, in accordance with the terms of the relevant Interchange Agreement, to the amount of that Transaction. Except in the circumstances specified in this IAC Code Set, Authorisation is effected online. ‘Authorised’ has a corresponding meaning.

“**Bank Identification Number**” and “**BIN**” means the registered identification number allocated by Standards Australia Limited in accordance with AS 3523 (also known as an Issuer Identification Number (IIN)).

“**Business Day**” means a day on which banks are open for general banking business in Sydney or Melbourne and on which the RITS is operating to process payments.

“**Card**” is defined in the IAC Regulations and means any card, device, application or identifier authorised by an Issuer, which is linked to an account or credit facility with the Issuer, for the purpose of effecting a Card Payment.

Last amended  
effective 1.1.20

“**Cardholder**” is defined in the IAC Regulations and means a customer of an Issuer who is issued with a Card and PIN or other authentication method or process.

Amended  
effective 1.1.20

“**Cardholder Data**” means any information that is stored on, or which appears on, a Card, and includes but it not necessarily limited to:

Inserted  
effective 1.1.16

- (a) Primary Account Number;
- (b) Cardholder Name;
- (c) Service Framework; and
- (d) Expiration Date.

“**Card Payment**” is defined in the IAC Regulations and means a Transaction under the rules of an Approved Card Payment System which is initiated by a Cardholder using a Card in Australia, irrespective of the infrastructure or network, including as the context requires, ATM Transactions, EFTPOS Transactions, Card-Not-Present Transactions and any adjustments in connection with those Transactions.

Last amended  
effective 1.1.20

**“Card Payment System”** is defined in the IAC Regulations and means, for the purposes of the IAC, the set of functions, procedures, arrangements, rules and devices that enable a Cardholder to effect a Card Payment with a third party other than the Card Issuer. For the avoidance of doubt, a Card Payment System may be a three-party scheme or a four-party scheme. Amended effective 1.1.20

**“Cash”** is defined in the IAC Regulations and means Australian legal tender. Amended effective 1.1.20

**“Certification”** is defined in the IAC Regulations and means in relation to an IA Participant initial certification or re-certification, in either case to the extent required by and in accordance with, Regulation 5.1(b) and f the IAC Code Set. Amended effective 1.1.20

**“Certification Checklist”** means in relation to an Acquirer, a checklist in the form of Annexure B.1 in IAC Code Set Volume 1 (Introduction and Member Obligations) and in relation to an Issuer, a checklist in the form of Annexure B.2 in IAC Code Set Volume 1 (Introduction and Member Obligations).

**“Certification Undertakings”** means all undertakings and representations given to the Company for the purposes of obtaining Certification. Inserted effective 1.1.16

**“Clearing/Settlement Agent”** means a Direct Clearer/Settler that clears and settles on behalf of Issuers and/or Acquirers which are not Direct Clearer/Settlers. Inserted effective 1.1.16

**“Clearing System”** is defined in the IAC Regulations and means a domestic payments clearing and settlement system established in accordance with the Constitution which is operated by, or under the auspices of, the Company. Amended effective 1.1.20

**“Closed Loop Cards”** means electronic payment cards that are restricted in terms of where they can be used at the time of purchase. Inserted effective 1.1.20

**“CNP Transaction”** means a transaction which is initiated by a Cardholder using a Card to make a purchase from a Merchant not in the same physical location. For example, over the internet (including via a mobile browser) or in an application. Inserted effective 1.07.19

**“Code”** and **“IAC Code”** is defined in the IAC Regulations and means: Amended effective 1.1.20

- (a) Volume 1 of the IAC Code Set (Introduction and Member Obligations);
- (b) Volume 2 of the IAC Code Set (Issuers Code);
- (c) Volume 3 of the IAC Code Set (Acquirers Code);
- (d) Volume 4 of the IAC Code Set (Device Requirements and Cryptographic Management);
- (e) Volume 5 of the IAC Code Set (Settlement Code);
- (f) Volume 6 of the IAC Code Set (ATM System Code);



- (g) Volume 7 of the IAC Code Set (Card Not Present Code); and
- (h) any other set of threshold industry standards or requirements for Card Payments which the IAF may adopt as industry standards or requirements for the purposes of these Regulations, from time to time.

**“Commencement Date”** is defined in the IAC Regulations and means, subject to IAC Regulation 1.6(b), 1 July 2015.

Amended effective 1.1.20

**“Committee of Management”** means the IAF.

Amended effective 1.1.20

**“Commercial off-the-shelf”** and **“COTS”** means a product that is designed for mass-market distribution and can be bought by any civilian entity, i.e. an unrestricted product not solely used by the military.

Inserted effective 1.1.19

**“Company”** means AusPayNet.

**“Compliance Date”** means 31 December 2016.

**“Compromised Terminal”** means a Terminal that has been tampered with for fraudulent purposes.

**“Constitution”** is defined in the IAC Regulations and means the constitution of AusPayNet as amended from time to time.

Amended effective 1.1.20

**“Corporations Law”** means the Corporations Act 2001 (Cth) and associated subordinate legislation as amended from time to time.

**“Counterfeit ATM Transaction”** means a fraudulent ATM Transaction initiated with a counterfeit copy of a chip Card.

**“Counterfeit ATM Transaction Chargeback Date”** [Deleted]

Deleted effective 3.7.17

**“Counterfeit ATM Transaction Claim”** means a claim by an Issuer under the indemnity in clause 4.5(c) (Liability Shift for Counterfeit ATM Transaction), made in the manner set out in clause 4.6 (Liability Shift Claim Process) of the IAC Code Set Volume 6 (ATM System Code).

Amended effective 3.7.17

**“Counterparty”** means the IA Participant direct settler (for example, an Issuer) identified in a File Settlement Instruction submitted by an Originator (for example, an Acquirer or Lead Institution), in accordance with this IAC Code Set and the requirements of the RITS Low Value Settlement Service.

**“Credit Items”** is defined in the IAC Regulations to include all credit payment instructions, usually electronically transmitted, which give rise to Interchange Activity, except as may be specifically excluded by the IAC Regulations or the IAC Code Set.

Amended effective 1.1.20

**“CVM”** means Cardholder Verification Method.

Inserted effective 20.8.18

**“Debit Chip Application”** means domestically issued debit chip application.

“**Debit Items**” is defined in the IAC Regulations to include all debit payment instructions, usually electronically transmitted, which give rise to Interchange Activity, except as may be specifically excluded by the IAC Regulations or the IAC Code Set.

Amended  
effective 1.1.20

“**Device Approval Applicant**” means:

Last amended  
effective 1.1.20

- (a) in relation to standard technologies (including SPoC solutions), the Sponsor, Acquirer, Third Party provider, device manufacturer or any third party who submits a device approval application; or
- (b) in relation to non-standard technologies, the Acquirer;

seeking approval of that device, solution or non-standard technology in accordance with Part 3 of IAC Code Set Volume 4.

“**Device Approval Process**” means the Device Approval Process for standard technologies and non-standard technologies published by AusPayNet, as updated from time to time, and a copy of which appears at Annexure G of IAC Code Set Volume 4.

Last amended  
effective 1.1.20

“**Direct Charge**” means a direct charge applied by an IA Participant under the Direct Charging Rules in Annexure F of IAC Code Set Volume 6 (ATM System Code).

Inserted  
effective 1.1.16

“**Direct Clearing/Settlement Arrangements**” means an arrangement between two indirectly connected IA Participants for the purposes of clearing and settlement with each other as Direct Clearer/Settlers.

Inserted  
effective 1.1.16

“**Direct Connection**” means a direct communications link between two IA Participants for the purposes of:

Inserted  
effective 1.1.16

- (a) exchanging ATM Transaction messages in respect of their own activities as an Issuer or as an Acquirer; and/or
- (b) exchanging ATM Transaction messages on behalf of other Issuers or Acquirers.

“**Direct Settler**” or “**Direct Clearer/Settler**” means:

Inserted  
effective 1.1.16

- (a) an Acquirer that is an IA Participant that:
  - (i) clears Items directly; and
  - (ii) settles directly, using its own ESA or using a means approved by the Management Committee,

with an Issuer, or with a representative of an Issuer appointed to settle on behalf of that Issuer for the value of payment obligations arising from Interchange Activities between it and that Issuer;

- (b) an Issuer that is an IA Participant that:
- (i) clears Items directly; and
  - (ii) settles directly, using its own ESA,
- with an Acquirer, or with a representative of an Acquirer appointed to settle on behalf of that Acquirer for the value of payment obligations arising from Interchange Activities between it and that Acquirer; or
- (c) a body corporate of the kind referred to in Volume 4 of the IAC Regulations, which represents one or more Acquirers or Issuers and, in such capacity, settles directly in accordance with Regulation 11.3(a) for the value of payment obligations arising from the Interchange Activities of those Acquirers or Issuers.

**“Disputed Transaction”** means an ATM Transaction:

Amended  
effective 1.1.16

- (a) which the Cardholder denies having initiated; or
- (b) where the ATM Transaction amount is claimed to be incorrect; or
- (c) in respect of which the ATM Operator Fee is claimed to be incorrect.

Inserted  
effective 1.1.16

Inserted  
effective 1.1.16

Inserted  
effective 1.1.16

**“Disruptive Event”** means any processing, communications or other failure of a technical nature, which affects, or may affect, the ability of any IA Participant to engage in Interchange Activity.

**“Double-length Key”** means a key of length 128 bits including parity bits or 112 bits excluding parity bits.

**“Doubtful ATM Transactions”** means those ATM Transactions which appear to have been successfully completed, although the ATM Transaction may not be recorded against the relevant Cardholder account.

Last amended  
effective  
21.11.16

**“EFT”** means Electronic Funds Transfer.

**“EFTPOS”** means Electronic Funds Transfer at Point of Sale.

**“EFTPOS PED”** [Deleted]

Deleted  
effective 20.8.18

**“EFTPOS Terminal”** means a Terminal for processing EFTPOS Transactions.

Inserted effective  
1.1.19

**“EFTPOS Transaction”** is defined in the IAC Regulations and means a Transaction conducted at a Merchant’s point of sale using a Terminal.

Last amended  
effective 1.1.20

**“EMV”** means the specifications as published by EMV Co. LLC.

**“EMV@ATM Terminal Standards”** means the standards and requirements set out in IAC Code Set Volume 6 (ATM System Code) Annexure G.

Amended  
effective 1.1.20

“**EMV Compliant**” in relation to an ATM Terminal means the ATM Terminal is certified by an Approved Evaluation Facility to be compliant with the EMV@ATM Terminal Standards.

“**EMV Phase 1**” means the transition arrangements through which a Transaction is created from the use of an EMV compliant Australian IC Card prior to the migration of the ATM system to full EMV functionality.

Amended  
effective 3.7.17

“**EMV Standards**” means:

- (a) in relation to Cards, the standards applicable to the Debit Chip Application loaded on the Card; and
- (b) in relation to ATM Terminals, means the standards set out in the IAC Code Set Volume 6 (ATM System Code) Annexure G EMV@ATM Terminal Standards.

Amended  
effective 1.1.20

“**Encapsulating Security Payload**” and “**ESP**” is a member of the IPsec protocol suite providing origin authenticity, integrity, and confidentiality protection of packets in tunnel mode, where the entire original IP packet is encapsulated, with a new packet header added which remains unprotected.

“**Encrypting PIN Pad**” and “**EPP**” means an approved device which is a component of a Terminal that provides secure PIN entry and cryptographic services to that Terminal.

“**ePayments Code**” means the code of conduct administered by the Australian Securities and Investments Commission.

“**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 Committee of Management.

“**Evaluation Facility**” [Deleted]

Deleted effective  
1.1.19

“**Evaluation Report**” means a report prepared by:

Last amended  
effective 1.1.20

- (a) an Approved Evaluation Facility; or
- (b) a laboratory authorised by the Company for the purpose of a non-standard technology;

under the Device Approval Process.

“**Exchange Settlement Account**” and “**ESA**” means an exchange settlement account, or similar account, maintained by a Framework Participant with the RBA used for, among other things, effecting settlement of inter-institutional payment obligations.

**“Fallback Transaction”** means an ATM Transaction initiated using a chip Card, which is processed and authorized by the Issuer using magnetic stripe data, in the circumstances described in IAC Code Set Volume 6 (ATM System Code) Annexure G.5.1.

Last amended  
effective 1.1.20

**“File Recall Instruction”** means a file in the format prescribed by the Reserve Bank of Australia and complying with the specifications for the RITS Low Value Settlement Service which can be accessed via a link on the Company’s extranet.

**“File Recall Response”** means a response to a File Recall Instruction, generated by the RITS Low Value Settlement Service.

**“File Settlement Advice”** means an advice in relation to a File Settlement Instruction, generated by the RITS Low Value Settlement Service.

**“File Settlement Instruction”** means a file in the format prescribed by the Reserve Bank and complying with the specifications for the RITS Low Value Settlement Service which can be accessed via a link on the Company’s extranet.

**“File Settlement Response”** means a response to a File Settlement Instruction, generated by the RITS Low Value Settlement Service.

**“Framework Participant”** is defined in the IAC Regulations and means a Constitutional Corporation:

Amended  
effective 1.1.20

- (a) which is deemed to be a Framework Participant pursuant to Regulation 4.4; or
- (b) whose Membership Application has been accepted pursuant to Regulation 4.3(f); and

in each case whose membership has not been terminated pursuant to Regulation 6.5.

**“Fraudulent CNP Transaction”** means a CNP Transaction which is also a Fraudulent Transaction.

Inserted  
effective 1.07.19

**“Fraudulent Transaction”** means a Transaction reported to an international card scheme as fraudulent which:

Inserted  
effective 1.07.19

- (a) includes but is not limited to unauthorised payment transactions and authorised payers acting dishonestly;
- (b) but excludes Transactions with Cards that were originally established using stolen or false identity information.

“**HMAC**” and “**Hash-based Message Authentication Code**” is a specific construction for calculating a message authentication code (MAC) involving a cryptographic hash function in combination with a secret key. HMACs are formed in conformance with AS2805.4.2 Electronic funds transfer—Requirements for interfaces Information technology -- Security techniques -- Message Authentication Codes (MACs) - Mechanisms using a dedicated hash-function.

“**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.

“**IA Participant**” is defined in the IAC Regulations and means a Framework Participant which is either:

Amended  
effective 1.1.20

- (a) an Issuer; or
- (b) an Acquirer; or
- (c) a body corporate which represents one or more Issuers or Acquirers and, in such capacity, settles directly in accordance with Regulation 11.3(a)(ii) for the value of the payment obligations arising from the Interchange Activities of those Acquirers or Issuers.

“**IAC**” is defined in the IAC Regulations and means the Issuers and Acquirers Community constituted by the IAC Regulations.

Amended  
effective 1.1.20

“**IAC Card Standards**” means the standards for Cards set out in the IAC Code Set Volume 2 (Issuer Code).

Amended  
effective 1.1.20

“**IAC Code Set**” is defined in the IAC Regulations and means the codes, practices, procedures, standards and/or specifications published pursuant to Regulation 11.1.

Amended  
effective 1.1.20

“**IAC Interchange Line**” means an Interchange Line that is not otherwise prescribed by an Approved Card Payment System.

Inserted  
effective 1.1.20

“**IAC Interchange Link**” means an Interchange Link that is not otherwise prescribed by an Approved Card Payment System.

Inserted  
effective 1.1.20

“**IAC Operational Broadcast**” means the form set out in IAC Code Set Volume 1 (Introduction and Member Obligations) Annexure D.

Amended  
effective 1.1.20

“**IAC Settlement Rules**” means the set of rules and requirements for the settlement of obligations arising as a result of exchange of Items set out in IAC Code Volume 5 (Settlement Code).

Amended  
effective 1.1.20

“**IAF**” or “**Issuers and Acquirers Forum**” is defined in the IAC Regulations and means the governing body for the IAC constituted by Part 7 of the IAC Regulations.

Amended  
effective 1.1.20

“**IC Card**” and “**ICC**” means a Card that contains an integrated circuit and that conforms to the EMV specifications.

“**Institutional Identifier Change Date**” means one of at least three dates in each calendar year specified by the IAF and notified by the Company to IA Participants prior to the commencement of that calendar year as being the Institutional Identifier Change Dates for that year.

Amended  
effective 1.1.20

“**Interchange**” means the exchange of Items for value between Acquirers and Issuers, via an Interchange Link, as a result of the use of an Issuer’s Card by a Cardholder to generate a Transaction. Interchange arrangements may, but need not, be reciprocal.

“**Interchange Activity**” is defined in the IAC Regulations and means:

Amended  
effective 1.1.20

- (a) the direct or indirect exchange of Items for value between Acquirers and Issuers, as a result of the use of an Issuer’s Card by a Cardholder to generate a Card Payment from facilities owned and/or operated by the Acquirer or a third party. Interchange arrangements may, but need not be, reciprocal; or
- (b) the exchange of Card Payment instructions and related messages between Acquirers and Issuers, pursuant to the rules of an Approved Card Payment System; or
- (c) any other Card-based electronic interchange activities from time to time approved for the purposes of this definition by the IAF.

“**Interchange Agreement**” means an agreement between an Acquirer and an Issuer that regulates the arrangements relating to Interchange Activity between them.

“**Interchange Fee**” means a fee charged to one party to an Interchange Activity by the other party to the Interchange Activity for access to its consumer electronic payments facilities.

“**Interchange Line**” means the physical communications infrastructure that provides the medium over which Interchange Activity is supported. An Interchange Line contains, at a minimum, one Interchange Link.

“**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 a triple-DES process.

“**Interchange Link**” means the logical link between an Acquirer and an Issuer which facilitates Interchange Activity between them. Interchange Links are supported physically by an Interchange Line, and are either direct between an Acquirer and Issuer or indirect via a third party intermediary.

**“Interchange Link Message Authentication”** means calculation and verification of the Message Authentication Code (MAC) that is being passed across an Interchange Link.

**“Interchange Link PIN Encryption”** means encryption of the PIN in accordance with ISO 9564.1 and IAC Code Set Volume 4 Clause 2.7(d)(i).

Amended  
effective  
21.11.16

**“Interchange Settlement Report”** means a report substantially in the form of Annexure A in IAC Code Set Volume 5 (Settlement Code).

**“Internet Key Exchange”** and **“IKE”** is the protocol used to set up a security association in the IPsec protocol suite.

**“ISO”** means an international standard as published by the International Standards Organization.

**“Issuer”** is defined in the IAC Regulations and means a Constitutional Corporation which, pursuant to the rules of an Approved Card Payment System, issues a Card to a Cardholder and, in connection with any Card Payment effected using that Card:

Amended  
effective 1.1.20

- (a) assumes obligations to the relevant Cardholder, which obligations are in the first instance discharged on its behalf by an Acquirer; and
- (b) engages, directly or indirectly, in Interchange Activity with that Acquirer as a result.

**“Issuer Authentication”** [Deleted]

Deleted  
effective 1.01.20

**“Issuer Fraud Rate”** means the aggregate of Fraudulent Transactions as calculated in accordance with the IAC Code Set Volume 7 (Card Not Present Code), clause 3.1.1.

Amended  
effective 1.01.20

**“Issuer Fraud Threshold”** means the maximum allowable Issuer Fraud Rate as set out at IAC Code Set Volume 7 (Card Not Present Code clause 3.1.1(b)).

Amended  
effective 1.01.20

**“Issuer Identification Number”** and **“IIN”** means a six digit number issued by ISO or Standards Australia that identifies the major industry and the card issuer. The IIN also forms the first part of the primary account number on the Card.

**“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 and possible different accessible linked accounts.

**“Items”** is defined in the IAC Regulations and means Credit Items or Debit Items.

Amended  
effective 1.1.20

**“Key Encrypting Key”** and **“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.



“**Key Loading Device/Key Injection Device**” and “**KLD/KID**” means a hardware device and its associated software that is used to inject keys into a Terminal.

Amended  
effective 29.4.16

“**Key Transfer Device**” and “**KTD**” means a hardware device that is used to transfer a cryptographic key between devices. Typically KTDs are used to transfer keys from the point of creation to Terminals in the field.

“**Lead Institution**” means a financial institution responsible for direct settlement of scheme payment obligations.

“**Letter of Approval**” means a letter, issued by the Company, approving the use of a Secure Cryptographic Device within IAC.

“**LVSS**” means the RITS Low Value Settlement Service.

“**LVSS BCP Arrangements**” means the contingency plan and associated documents published by the Reserve Bank of Australia for the purposes of the RITS Low Value Settlement Service, and which can be accessed via a link on the Company’s extranet.

“**LVSS Contact**” means the person nominated by a IA Participant as its primary contact for LVSS inquiries, as listed on the Company’s extranet.

“**Merchant**” means a person which:

Amended  
effective 1.1.19

- (a) supplies goods or services to a Cardholder; and
- (b) has an agreement with an Acquirer to process and settle Card Payments.

“**Merchant Fraud Rate**” means the aggregate of Fraudulent Transactions as calculated in accordance with IAC Code Set Volume 7 (Card Not Present Code), clause 3.3.2(a).

Amended  
effective 1.01.20

“**Merchant Fraud Threshold**” means the maximum allowable Merchant Fraud Rate as set at IAC Code Set Volume 7 (Card Not Present Code), clause 3.3.2(b).

Amended  
effective 1.01.20

“**Message Authentication Code**” and “**MAC**” 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 conformance with AS 2805.4.

Amended  
effective 20.8.18

“**Nine AM (9am) Settlement**” means the multilateral settlement of obligations arising from previous days’ clearings of low value payments which occurs in RITS at around 9am each business day that RITS is open.

“**NODE**” or “**Node**” means a processing centre such as an Acquirer, an Issuer, or an intermediate network facility.

**“Non-standard POI Technology”** means a POI solution/technology that by nature of its design is unable to meet certain Australian or global payment standards identified in IAC Code Set Volume 4 (Device Requirements) Annexure G Schedule 1.

Inserted  
effective 1.1.20

**“Notice of Standard – Merchant Pricing for Credit, Debit and Prepaid Card Transactions”** is the informative guide referred to in clause 2.1.2 and set out in Annexure F to the IAC Code Set Volume 1 (Introduction and Member Obligations) relating to the notification requirements in the Reserve Bank’s Scheme Rules relating to Merchant Pricing for Credit, Debit and Prepaid Card Transactions (Standard No. 3 of 2016).

Inserted  
effective 1.6.17

**“On-us Transactions”** means Transactions that do not traverse Interchange and where the Acquirer and card Issuer are the same entity.

Inserted  
effective 1.1.20

**“Originator”** means the party (for example an Acquirer direct settler or Lead Institution) which, as a result of either acquiring a Transaction or, in the case of a Lead Institution, by arrangement, is responsible for the submission of a File Settlement Instruction in accordance with this IAC Code Set and the requirements of the RITS Low Value Settlement Service.

**“Operator Member”** is defined in the IAC Regulations and means a Constitutional Corporation which:

Amended  
effective 1.1.20

- (a) has been admitted, or which is eligible for admission, to membership of the Company pursuant to Article 2.11 of the Constitution;
- (b) is the operator or administrator of an Approved Card Payment System; and
- (c) is determined by the IAF to meet the Approval Criteria for Operator Members.

**“Partial Dispense”** means a Transaction that results in an amount of Cash being dispensed from an ATM that is less than the amount requested by the Cardholder.

**“PCISSC”** means the Payment Card Industry Security Standards Council.

Amended  
effective 20.8.18

**“PCI Evaluation Report”** means an Evaluation Report, prepared in respect of the requirements set out in PCI PTS published standards. (PCI standards can be found at <https://www.pcisecuritystandards.org>).

Amended  
effective 1.1.19

**“PCI Plus Evaluation Report”** means an Evaluation Report, prepared in respect of the PCI Plus Requirements, and if applicable, includes any delta report prepared in respect of the device.

Amended  
effective 1.1.19

**“PCI Plus Requirements”** means the requirements set out in IAC Code Set Volume 4 (Device Requirements and Cryptographic Management) Annexure B which are determined by the Company to be additional to the requirements of PCI PTS.

Last amended  
effective 1.1.20

“**PCI Points**” means the attack potential calculated in accordance with Appendix B of the Payments Card Industry (PCI) document “PCI PIN Transaction Security Point of Interaction Modular Derived Test Requirements”.

Amended effective 1.1.20

“**PED**” means a PIN Entry Device.

“**Physically Secure Device**” means a device meeting the requirements specified in AS 2805.14.1 for a physically secure device. Such a device, when operated in its intended manner and environment, cannot be successfully penetrated or manipulated to disclose all or part of any cryptographic key, PIN, or other secret value resident within the device. Penetration of such a device shall cause the automatic and immediate erasure of all PINs, cryptographic keys and other secret values contained within the device.

Amended effective 21.11.16

“**PIN**” is defined in the IAC Regulations and means a personal identification number which is either issued by an Issuer, or selected by a Cardholder for the purpose of authenticating the Cardholder by the Issuer of the Card.

Amended effective 1.1.20

“**PIN Entry Device**” and “**PED**” means a component of a Terminal which provides for the secure entry and encryption of PINs in processing a Transaction.

“**POI**” means Point Of Interaction technologies that can be provided to a Merchant to undertake Card Payments. POI technologies include attended and unattended Point of Sale (POS) devices and ATMs.

Inserted effective 1.1.16

“**POS**” means Point of Sale.

Inserted effective 1.1.19

“**Prepaid Card**” means a Card that:

- (a) enables the Prepaid Cardholder to initiate electronic funds transfers up to a specified amount (subject to any other conditions that may apply); and
- (b) draws on funds held by the Prepaid Program Provider or third party by arrangement with the Program Provider (as opposed to funds held by the Prepaid Cardholder).

The definition of a Prepaid Card extends to both single use and 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.

“**PVC**” means Public Key Verification Code.

Inserted effective 20.8.18

“**Quarter**” means the unit of 3 months commencing on either 1 January, 1 April, 1 July or 1 October.

Inserted  
effective 1.07.19

“**Recognised APS**” is defined in the IAC Regulations and has the meaning given in the Constitution.

Amended  
effective 1.1.20

“**Record of Transaction**” has the meaning given in the ePayments Code and IAC Code Set Volume 3 (Acquirer Code).

“**Regulations** or the “**IAC Regulations**” is defined in the IAC Regulations and means the regulations for IAC (including, without limitation, the annexures and schedules to the Regulations) as amended from time to time. A reference to a particular Regulation has a corresponding meaning.

Amended  
effective 1.1.20

“**Remote Management Solution**” and “**RMS**” means a solution comprising both hardware and software which connects to an SCM over a network and provides access to an SCM while it is in a sensitive state.

“**Reporting Date**” means the 15th day of the month which follows the end of each Quarter, being 15 April, 15 July, 15 October or 15 January. If the 15th day of the month occurs on a weekend, the Reporting Date for that month will be the first business day following the 15th day.

Inserted  
effective 1.07.19

“**Reserve Bank**” means the Reserve Bank of Australia.

“**Retained Card**” in relation to an ATM Transaction, has the meaning given in clause 2.8 of IAC Code Set Volume 6 (ATM System Code).

“**Risk Based Analysis**” has the meaning given to it in IAC Code Set Volume 7 (Card Not Present Code), clause 2.1.1.

Amended  
effective 1.01.20

“**RITS**” means the Reserve Bank Information and Transfer System.

“**RITS Low Value Settlement Service**” means the Reserve Bank’s settlement file transfer facility which must be used by:

- (a) each Acquirer and Lead Institution to submit File Settlement Instructions and associated File Recall Instructions; and
- (b) each Acquirer, Lead Institution and Issuer, if it so elects, to receive File Settlement Advices, File Settlement Responses and File Recall Responses.

“**RITS Regulations**” means the regulations for RITS published by the Reserve Bank of Australia.

“**SCD Security Standards**” in relation to an SCD, means the standards from time to time published in IAC Code Set Volume 4 (Device Requirements and Cryptographic Management), Part 2.

Last amended  
effective 1.1.20

- “**SCM**” means a Security Control Module sometimes referred to as a Hardware Security Module (HSM). Amended effective 20.8.18
- “**Secretary**” is defined in the IAC Regulations and means a person appointed by the Chief Executive Officer to perform the duties of secretary of the IAF under Regulation 7.14. Amended effective 1.1.20
- “**Secure Card Reader PIN**” and “**SCR**” means a physical card reader that has been approved by PCI PTS and is a component of a SPOC Solution. Inserted effective 1.1.19
- “**Secure Cryptographic Device**” and “**SCD**” means a device that provides physically and logically protected cryptographic or PIN handling services and storage e.g., EPP, Terminal, Key Injection Device or hardware security module. Amended effective 20.8.18
- “**Security Control Module**” and “**SCM**” means a physically and logically protected hardware device that provides an intentionally limited set of secure cryptographic services. Amended effective 1.1.19
- “**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 Items**” is defined in the IAC Regulations and means, Items which are either: Amended effective 1.1.20
- (a) ATM Transactions cleared under the auspices of the IAC Code Set Volume 6 (ATM System Code); or
  - (b) EFTPOS Transactions cleared pursuant to the Rules prescribed for the EFTPOS Card Payment System (as defined in those Rules) by the administrator of that system; or
  - (c) credit payment instructions referable to a transaction of the type described in paragraphs (a) and (b).
- “**Software-based PIN entry on COTS**” and “**SPoC**” means the term Software-based PIN entry on COTS as used in the PCISSC SPoC standards. Inserted effective 1.1.19
- “**Sponsor**” means the Acquirer which, as among all Acquirers for a Terminal, is taken to be the lead Acquirer for that Terminal, with ultimate responsibility for the integrity and security of software and encryption keys for Transactions involving that Terminal. Amended effective 20.8.18
- “**Standard Interchange Specification**” means the technical specification set out in Annexure A of IAC Code Set Volume 6 (ATM System Code). Inserted effective 1.1.16

**“Statistically Unique”** means an acceptably low statistical probability of an entity being duplicated by either chance or intent. Technically, statistically unique is defined as follows:

*“For the generation of n-bit quantities, the probability of two values repeating is less than or equal to the probability of two n-bit random quantities repeating. Thus, an element chosen from a finite set of 2n elements is said to be statistically unique if the process that governs the selection of this element provides a guarantee that for any integer  $L \leq 2n$  the probability that all of the first L selected elements are different is no smaller than the probability of this happening when the elements are drawn uniformly at random from the set.”*

**“Strong Customer Authentication”** or **“SCA”** has the meaning given to it in IAC Code Set Volume 7 (Card Not Present Code), clause 2.1.2.

Amended  
effective 1.01.20

**“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 subjected to any feasible attack. A Tamper-responsive SCM must comply with the requirements of IAC Code Set Volume 4 (Device Requirements and Cryptographic Management).

**“Terminal”** means an electronic device which can be used to initiate a Transaction e.g. ATM, UPT or EFTPOS Terminal.

Last amended  
effective 1.1.19

**“Terminal Identification Number”** means the unique identification 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.

**“Third Party Provider”** means a body corporate which provides an outsourced facility to a IA Participant for any function involving:

- (a) interchange;
- (b) PIN processing;
- (c) transaction processing;
- (d) key management; or
- (e) any other service which directly or indirectly supports any of the functions described in clauses (a) to (d) above.

**“Threshold Requirement”** is defined in the IAC Regulations and means a requirement under the IAC Regulations or in this IAC Code Set which the IAF determines to be so fundamental to the integrity and safety of Card Payments that compliance is to be enforceable by imposition of a fine under Regulation 6.2, the details of which are published on the Company’s extranet.

Amended  
effective 1.1.20

**“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 AS 3524-2008, excluding start sentinel, end sentinel and Longitudinal Redundancy Check.

**“Transaction”** is defined in the IAC Regulations and means an electronic funds transfer, cash withdrawal or other transaction initiated by a Cardholder using a Card which allows for the accessing of available funds held in an account, or a credit facility linked to an account, or account information.

Last amended  
effective 1.1.20

**“Triple-DES”** means the encryption and decryption of data using a defined compound operation of the DEA-1 encryption and decryption operations. Triple-DES is described in AS2805.5.4.

**“Unattended Device”** means a device intended for principal deployment in a location not subject to the regular day-to-day oversight by a trusted employee of the Acquirer or their trusted agent.

**“Unattended Payment Terminal”** and **“UPT”** means a Terminal intended for deployment in an EFTPOS network without Merchant oversight.

**Next page is 2.1**

---

## PART 2 ANALYSIS AND AUTHENTICATION

Amended  
effective 1.1.20

### 2.1 Analysis and Authentication Types

Amended  
effective 1.1.20

#### 2.1.1 *Risk Based Analysis*

Risk Based Analysis is a method that adapts the rigorousness of Cardholder identity verification and device authentication processes to the risk that is associated with the CNP Transaction, based on the characteristics of the Cardholder's interaction with the Merchant, including, but not limited to, the Cardholder's:

Amended  
effective 1.1.20

- (a) geo-location;
- (b) IP address;
- (c) device type;
- (d) time; and
- (e) transaction pattern.

#### 2.1.2 *Strong Customer Authentication (“SCA”)*

SCA is an authentication method in which the Cardholder's identity is verified with at least two of the following independent factors:

- (a) Knowledge factor; something only the Cardholder knows, including, for example, a password, a passphrase, an answer to a secret question, or a PIN;
- (b) Possession factor; something only the Cardholder possesses, including, for example, a credit card, a hardware token, or a smartphone; or
- (c) Inherence factor; something the Cardholder is, including, for example, a biometric feature such as a fingerprint scan, an iris scan, or facial recognition; or a behavioral feature such as type or swipe dynamics.

*Note: SCA may also be known as ‘strong authentication’, ‘two-factor authentication’ (2FA) or ‘multi-factor authentication’ (MFA).*

Amended  
effective 1.1.20

### 2.2 Exempt Transactions

Amended  
effective 1.1.20

A transaction which is an Exempt Transaction for the purposes of SCA is any of the following:

Amended  
effective 1.1.20

- (a) Recurring Transaction, as set out in clause 2.2.2;
- (b) Trusted Customer Transaction, as set out in clause 2.2.3; or

Amended  
effective 1.1.20Amended  
effective 1.1.20



- (c) Wallet Transaction, as set out in clause 2.2.4;

Amended effective 1.1.20

except in either of the following circumstances:

- (d) the Cardholder changes the Card to another Card that has not been previously used; or
- (e) more than 180 days have passed since the Cardholder accessed the online service.

**2.2.1 Recurring Transaction**

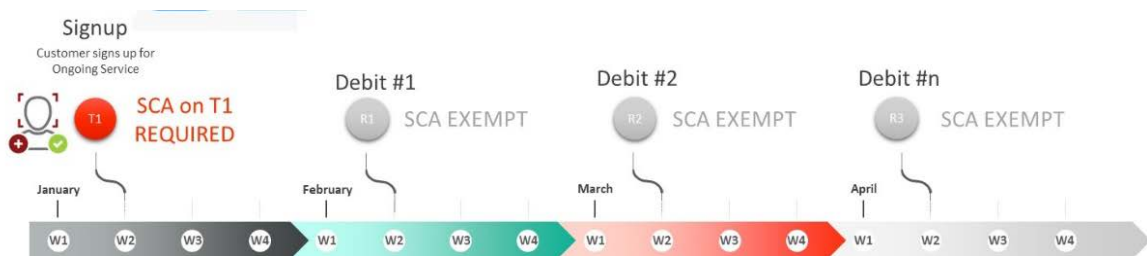
A “Recurring Transaction” is a CNP Transaction which occurs within a recurring series of CNP Transactions between a Merchant and Cardholder (which may be of a variable value) which the Merchant is authorised to conduct because that Cardholder has consented by:

Amended effective 1.1.20

- (a) acceptance of the Merchant’s terms and conditions for that recurring series, which recurring series ends upon a change to those terms and conditions;
- (b) being notified of, and proceeding with the Merchant’s commercial terms for payment amount, date and communication method in respect of that recurring series, which recurring series ends upon a change to those commercial terms; or
- (c) providing verifiable consent, where the Cardholder’s consent is retained on file by the Merchant;

but does not include the first CNP Transaction in each recurring series.

*Note: The diagram below illustrates the points at which a Recurring Transaction will be an Exempt Transaction.*



**2.2.2 Trusted Customer Transaction**

A “Trusted Customer Transaction” is a subsequent CNP Transaction conducted by a customer with a Merchant, where:

Amended effective 1.1.20

- (a) the Merchant has previously identified the customer; and

- (b) the Merchant identifies the following credentials in relation to that customer during the subsequent transaction:
- (i) either the:
    - (A) customer logs into a customer account; or
    - (B) customer uses an assigned merchant token; and
  - (ii) the Card used by the customer for the subsequent transaction is the same Card on file used previously with the Merchant; and
  - (iii) either the:
    - (A) customer undertakes the subsequent transaction using the same device ID used by that customer in a previous transaction with the Merchant; or
    - (B) customer uses the same delivery address, mobile number, or email address during the subsequent transaction as in a previous transaction with the Merchant.

*Note:*

- (i) *The assigned merchant token can be either an EMV payment token or a payment token adopted by the merchant as a PAN replacement or unique customer identifier.*
- (ii) *The diagram below illustrates the points at which a Trusted Customer Transaction will be an Exempt Transaction.*



### 2.2.3 **Wallet Transactions**

“Wallet Transactions” are CNP Transactions conducted through a digital or mobile wallet in which one or more of the following steps are, or have been, required:

Amended effective 1.1.20

- (a) Cardholder identity verification - Cardholder has been requested to provide upfront identity verification to load a Card into a wallet, combined with the tokenisation of the credential; and

Amended effective 1.1.20

- (b) Transaction authorisation - the wallet requires a device that has been previously verified (with a token) to use biometrics or a passcode for the Cardholder to authorise each Transaction.

**Next page is 3.1**

## PART 3 IAC PARTICIPANT OBLIGATIONS

The obligations in Part 3 commence for all current Issuers and Acquirers on 1 July 2019.

Any Issuer or Acquirer who becomes a member of the IAC after 1 July 2019, will be subject to the obligations in Part 3 from the first day of the first Quarter commencing after that Issuer or Acquirer becomes an IAC Participant.

### 3.1 Obligations on Issuers

Amended  
effective 1.1.20

- (a) An Issuer must calculate its Issuer Fraud Rate for the preceding Quarter in accordance with clause 3.1.1(a).
- (b) Upon receipt by the Issuer of a request for SCA from a Merchant, Payment Gateway or Acquirer (the “requested transaction”):
  - (i) the Issuer must perform SCA on the requested transaction if that Issuer’s Fraud Rate breached the Issuer Fraud Threshold for the preceding two consecutive Quarters except where the requested transaction is an Exempt Transaction; and
  - (ii) for any Issuer to whom clause 3.1(b)(i) does not apply, it is at the Issuer’s discretion to perform either Risk Based Analysis or SCA on the requested transaction.
- (c) An Issuer must submit to AusPayNet any information required in clause 3.2.1.

*Note: It is recommended, but not mandatory, that Issuers notify Cardholders when their Card is being used for a CNP transaction using the Cardholder’s registered mobile phone number (SMS or phone call), mobile or desktop app (via push notifications) or email address. Parameters can also be set to ensure notifications are only sent to the Cardholder if a transaction meets certain restrictions (e.g. all CNP transactions over \$100). Issuers can set Cardholder notifications as an opt-in or opt-out service.*

#### 3.1.1 Issuer Fraud Rate and Threshold

Amended  
effective 1.1.20

- (a) The formula for calculation of the Issuer Fraud Rate is:

$$\text{Issuer Fraud Rate (basis points)} = \frac{\text{VALUE}_F}{\text{VALUE}_T} \times 10,000$$

Where:

- (i) VALUE<sub>F</sub> in the Issuer Fraud Rate calculation is the total amount of that Issuer's settled, Fraudulent CNP Transactions, that were passed through to the Issuer for SCA (irrespective of whether the Issuer performed requested SCA), including Exempt Transactions and less any Out of Scope Transactions, in the relevant Quarter for which the calculation is conducted.

*Note: The definition of Fraudulent CNP Transaction means it is to be calculated in the same Quarter for which it is reported to the card scheme.*

- (ii) VALUE<sub>T</sub> in the Issuer Fraud Rate calculation is the total amount of all of the Issuer's settled, CNP Transactions, that were passed through to the Issuer for SCA (irrespective of whether the Issuer performed requested SCA), including any Exempt Transactions and less any Out of Scope Transactions, in the relevant Quarter for which the calculation is conducted.

- (b) The Issuer Fraud Threshold is set at 15 basis points.
- (c) An Issuer is in breach of the Issuer Fraud Threshold if it has an Issuer Fraud Rate of 15 basis points or higher in any one Quarter.

### 3.1.2 **Issuer Compliance**

Amended  
effective 1.1.20

- (a) Where an Issuer breaches the Issuer Fraud Threshold in two consecutive Quarters, that Issuer must perform SCA on all CNP Transactions in accordance with clause 3.1(b)(i), until the Issuer's Fraud Rate for a Quarter no longer breaches the Issuer Fraud Threshold.
- (b) It is a Threshold Requirement that an Issuer not breach the Issuer Fraud Threshold for three consecutive Quarters.

Amended  
effective 1.1.20

*Note: An Issuer should take measures to reduce their Fraud Rate after breaching the Issuer Fraud Threshold for a Quarter.*

### 3.1.3 **Issuer Reporting**

Amended  
effective 1.1.20

- (a) On or before each Reporting Date, an Issuer is to provide to AusPayNet any information from the preceding Quarter required by clause 3.1.3(b).
- (b) An Issuer must provide, for each Quarter, the following information to AusPayNet in writing (in AUD where required) using the Template Reporting form as set out in clause 5.1:
  - (i) value of Fraudulent CNP Transactions that were passed through to the Issuer for SCA (irrespective of whether the Issuer performed requested SCA);

Amended  
effective 1.1.20

Amended  
effective 1.1.20

Amended  
effective 1.1.20

- (ii) value of all CNP Transactions that were passed through to the Issuer for SCA (irrespective of whether the Issuer performed requested SCA);
- (iii) value of Fraudulent CNP Transactions that were not passed through to the Issuer for SCA;
- (iv) value of all CNP Transactions that were not passed through to the Issuer for SCA;
- (v) value of all Fraudulent CNP Transactions;
- (vi) value of all CNP Transactions;
- (vii) value of all Fraudulent Transactions which are MOTO;
- (viii) value of all Transactions which are MOTO; and
- (ix) its Issuer Fraud Rate (bps).

*Note:*

Amended  
effective 1.1.20

- (i) *Reporting at 3.3(b)(i) to 3.3(b)(vi) excludes MOTO as it is an Out of Scope Transaction.*

### 3.2 Obligations on Acquirers

Amended  
effective 1.1.20

An Acquirer must:

Inserted  
effective 1.1.20

- (a) calculate the Merchant Fraud Rate for the preceding Quarter for each of their Merchants (per Merchant ID) in accordance with clause 3.2.1(a);
- (b) if requested by their Merchant, notify that Merchant of their Merchant Fraud Rate for the preceding Quarter;
- (c) on or before each Reporting Date, notify any of their Merchants whose Merchant Fraud Rate exceeds the Merchant Fraud Threshold for a Quarter, of that fact;
- (d) take any steps required by clause 3.2.2; and
- (e) submit to AusPayNet any information required in clause 3.2.3.

*Note: While not mandatory, it is recommended that Acquirers notify each Merchant of their Merchant Fraud Rate for the preceding Quarter and assist them in lowering their Merchant Fraud Rate.*

### 3.2.1 *Merchant Fraud Rate and Threshold*

- (a) The formula for calculation of the Merchant Fraud Rate is:

$$\text{Merchant Fraud Rate (basis points)} = \frac{\text{VALUE}_F}{\text{VALUE}_T} \times 10,000$$

Where:

Amended  
effective 1.1.20

- (i) VALUE<sub>F</sub> in the Merchant Fraud Rate calculation is the total amount of that Merchant's settled, Fraudulent CNP Transactions including Exempt Transactions and less the value of any:
- (A) Out of Scope Transactions; and
  - (B) CNP Transactions that were passed through to the Issuer for SCA (irrespective of whether the Issuer performed requested SCA);

in the relevant Quarter for which the calculation is conducted.

*Note: A Fraudulent CNP Transaction is to be included in the same Quarter for which it is reported to the card scheme.*

- (ii) VALUE<sub>T</sub> in the Merchant Fraud Rate calculation is the total amount of that Merchant's settled, CNP Transactions including any Exempt Transactions and less any Out of Scope Transactions, in the relevant Quarter for which the calculation is conducted.
- (b) The Merchant Fraud Threshold is set at:
- (i) 20 basis points; and
  - (ii) the amount in VALUE<sub>F</sub> of the Merchant Fraud Rate being \$50,000
- (c) An Acquirer's Merchant exceeds the Merchant Fraud Threshold for any one Quarter, if:
- (i) the Merchant Fraud Rate is 20 basis points or higher; and
  - (ii) the amount in VALUE<sub>F</sub> of the Merchant Fraud Rate is \$50,000 or higher.

**3.2.2 Acquirer Compliance**Amended  
effective 1.1.20

- (a) Where an Acquirer's Merchant exceeds the Merchant Fraud Threshold for one Quarter, that Acquirer must notify the Merchant that:
  - (i) the Merchant has exceeded the Merchant Fraud Threshold; and
  - (ii) the Merchant should take measures to reduce their Merchant Fraud Rate.
- (b) Where an Acquirer's Merchant exceeds the Merchant Fraud Threshold for two consecutive Quarters, that Acquirer must require the Merchant to perform SCA on all CNP Transactions, other than Exempt Transactions, until the Merchant's Fraud Rate for a Quarter no longer exceeds the Merchant Fraud Threshold.

*Note: Where a Merchant exceeds the Merchant Fraud Threshold for three consecutive Quarters, it is recommended (but not required) that the Merchant pass all CNP Transactions through to the Issuer for SCA (however, it is at the Issuer's discretion whether to perform SCA).*

- (c) It is a Threshold Requirement that an Acquirer's Merchant not exceed the Merchant Fraud Threshold for four consecutive Quarters.

**3.2.3 Acquirer Reporting**Amended  
effective 1.1.20

- (a) On or before each Reporting Date:
  - (i) an Acquirer is to provide to AusPayNet any information from the preceding Quarter required by clause 3.2.3(b);
  - (ii) a self-Acquirer is to provide to AusPayNet any information from the preceding Quarter required by clause 3.2.3(c) and 3.2.3(c).
- (b) An Acquirer must, for each Quarter, provide the following information to AusPayNet in writing (in AUD where required):
  - (i) Merchant Breach Report: The following information for each Merchant who has exceeded the Merchant Fraud Threshold in that Quarter:
    - (A) Merchant ID (or scheme-supplied aggregated Merchant code);
    - (B) Merchant Category Code (MCC);
    - (C) Value of CNP Transactions;
    - (D) Value of Fraudulent CNP Transactions; and

Amended  
effective 1.1.20Amended  
effective 1.1.20



- (E) Merchant Fraud Rate calculation (bps).
- (ii) The following information is required from those Acquirers who are in partnership with self-Acquirers. Amended effective 1.1.20
- (A) All scheme-assigned aggregated Merchant Codes, per self-Acquirer; and Amended effective 1.1.20
- (B) The information required at clause 3.2.3(b)(i), regardless of whether the self-Acquirer has exceeded the Merchant Fraud Threshold. Amended effective 1.1.20

*Note: Where previously agreed with AusPayNet, those Merchants that are also considered as 'payment facilitators' are to provide the Merchant Breach Report and Acquirer Trend Report for their sub-merchants, each Quarter. To avoid duplication, these Merchants (payment facilitators) must ensure their Acquirer excludes their data from their Acquirer's reports.*

- (iii) An Acquirer Trend Report: For each of the following Merchant Fraud Rate categories:
- (A) <1 bps;
- (B) 1 to <5 bps;
- (C) 5 to <10 bps;
- (D) 10 to <15 bps;
- (E) 15 to <20 bps;
- (F) 20 to <25 bps;
- (G) 25 to <30 bps;
- (H) 30 to <35 bps;
- (I) 35 to <40 bps; and
- (J) >40 bps;
- provide the following information:
- (K) Number (count) of merchants in that Merchant Fraud Rate category;
- (L) value of Fraudulent CNP Transactions;
- (M) value of all CNP Transactions;

- (N) value of fraudulent MOTO transactions;
- (O) value of all MOTO transactions;
- (P) volume (count) of Fraudulent CNP Transactions;
- (Q) volume (count) of all CNP Transactions;
- (R) volume (count) of Fraudulent Transactions which are MOTO;
- (S) volume (count) of all Transactions which are MOTO; and
- (T) average Merchant Fraud Rate for that category.

**Note:**Amended  
effective 1.1.20

- (i) *Reporting at clause 3.2.3(b)(iii) excludes MOTO transactions unless MOTO is specifically referred to as CNP Transactions conducted by MOTO are Out of Scope.*
- (ii) *Template reporting forms to be used by Acquirers in providing the above information is at clause 5.2 and 5.3.*
- (iii) *The ‘Acquirer Trend Report’ will be used by AusPayNet to monitor the impact of the CNP Framework and conduct reviews.*
- (c) A self-Acquirer must, for each Quarter, provide the following information to AusPayNet in writing (in AUD where required):
  - (i) All scheme-assigned aggregated Merchant Codes, per Acquirer;
  - (ii) The information listed at clause 3.2.3(b)(i), using eftpos transaction data only.

Amended  
effective 1.1.20**Next page is 4.1**

## **PART 4 THRESHOLD REQUIREMENTS AND SANCTIONS**

Breaches of Threshold Requirements will follow the processes contained in the Sanctions Rules.

**Next page is 5.1**

## **PART 5 APPENDICES**

### **5.1 Issuer Report Template**

**Report header:** Issuer Name and ID, reporting period, USD-AUD exchange rate used (if required).

Field ID	Field Name	Type	Value / Units	Field Definition
1	EcommAuthFraud	Numeric	AUD	Value of all fraudulent settled, CNP Transactions that were passed through to the Issuer for SCA, irrespective of whether the Issuer performed requested SCA (excluding MOTO)
2	EcommAuthTotal	Numeric	AUD	Value of all (fraudulent + genuine) settled, CNP Transactions that were passed through to the Issuer for SCA, irrespective of whether the Issuer performed requested SCA (excluding MOTO)
3	EcommNoAuthFraud	Numeric	AUD	Value of all fraudulent settled, CNP Transactions that were not passed through to the Issuer for SCA (excluding MOTO)
4	EcommNoAuthTotal	Numeric	AUD	Value of all (fraudulent + genuine) settled, CNP Transactions that were not passed through to the Issuer for SCA (excluding MOTO)
5	EcommAllFraud	Numeric	AUD	Value of all fraudulent settled, CNP Transactions, regardless of whether passed through to Issuer for SCA and regardless of whether the Issuer performed requested SCA (excluding MOTO)
6	EcommAllTotal	Numeric	AUD	Value of all (fraudulent + genuine) settled, CNP Transactions, regardless of whether passed through to Issuer for SCA and regardless of whether the Issuer performed requested SCA (excluding MOTO)
7	MOTOFraud	Numeric	AUD	Value of all fraudulent settled MOTO transactions
8	MOTOTotal	Numeric	AUD	Value of all (fraudulent + genuine) settled MOTO transactions
9	IssuerFraudRate	Numeric	Basis points	Fraud Rate calculation: (Field #1 / Field #2) x10000

## 5.2 Merchant Breach Report Template

**Report header:** Acquirer name and ID, reporting period, USD-AUD exchange rate used (if required).

Field ID	Field Name	Type	Value / Units	Field Definition
1	MerchantID	Alpha-numeric	-	Acquirer-assigned Merchant ID or, where applicable, Scheme-assigned aggregated Merchant Code
2	MCC	Numeric	-	Merchant Category Code
3	ValueEcommFraud	Numeric	AUD	Value of all fraudulent settled, CNP Transactions (excluding MOTO)
4	ValueEcommTotal	Numeric	AUD	Value of all (fraudulent + genuine) settled, CNP Transactions (excluding MOTO)
5	MerchantFraudRate	Numeric	Basis points	Fraud Rate calculation: (Field #3 / Field #4) x10000

### 5.3 Acquirer Trend Report Template

**Report header:** Acquirer name and ID, reporting period, USD-AUD exchange rate used (if required).

Field ID	Field Name	Type	Value / Units	Field Definition
1	FraudRateCategory	Alpha-numeric	-	Fraud Rate Category*
2	NumberofMerchants	Numeric	-	Number of merchants that fit into each category
3	ValueEcommFraud	Numeric	AUD	Value of all fraudulent settled, CNP Transactions (excluding MOTO)
4	ValueEcommTotal	Numeric	AUD	Value of all (fraudulent + genuine) settled, CNP Transactions (excluding MOTO)
5	ValueMOTOFraud	Numeric	AUD	Value of all fraudulent settled, MOTO transactions
6	ValueMOTOTotal	Numeric	AUD	Value of all (fraudulent + genuine) settled, MOTO transactions
7	VolumeEcommFraud	Numeric	Txns	Number (count) of all fraudulent settled, CNP Transactions (excluding MOTO)
8	VolumeEcommTotal	Numeric	Txns	Number (count) of all (fraudulent + genuine) settled, CNP Transactions (excluding MOTO)
9	VolumeMOTOFraud	Numeric	Txns	Number (count) of all fraudulent settled, MOTO transactions
10	VolumeMOTOTotal	Numeric	Txns	Number (count) of all (fraudulent + genuine) settled, MOTO transactions
11	AvgFraudRate	Numeric	Basis points	Fraud Rate calculation: (Field #2 / Field #3) x10000

**\* Fraud Rate Categories:**

- <1 bps
- 1 to <5 bps
- 5 to <10 bps
- 10 to <15 bps

- 15 to <20 bps
- 20 to <25 bps
- 25 to <30 bps
- 30 to <35 bps
- 35 to <40 bps
- >40 bps

**End**