Effective:
1 January 2024
Version 017

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

Australian Payments Network Limited
Telephone: (02) 9216 4888

Code Set for

ISSUERS AND ACQUIRERS COMMUNITY FRAMEWORK

Volume 7
Card Not Present Code

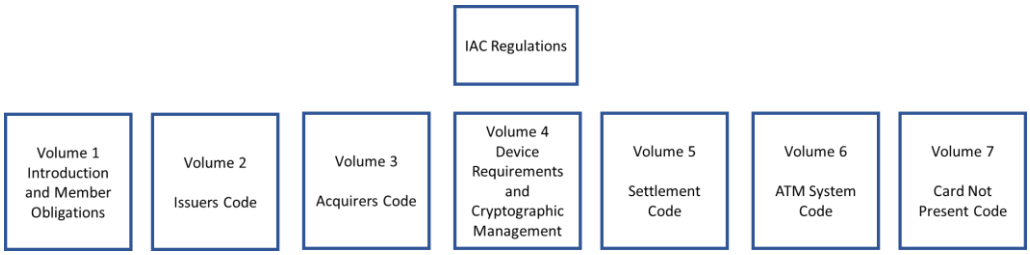
INDEX

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 and manual entry; and[1]

[1] Last amended effective 29/8/22, version 014 r&p 001.22

(b) CNP Transactions in which the card used is a corporate card, gift card or Prepaid Card. [2]

(i) A corporate card is a card issued to a company and at the company's request to certain employees that enables the cardholder to undertake transactions and is intended to be used for commercial purposes, commonly travel and entertainment expenses.

(ii) A gift card is a debit card that is loaded with an amount of money and may be used to purchase goods or services up to the value of the loaded amount.

Note: The following, by definition and application of this Code in clause 1.2 are also Out of Scope Transactions:[3]

(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.

(d) 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

Definitions are located in a separate document entitled 'Interpretation & Definitions'.

Next page is Part 2

[2] Amended effective 29/8/22, version 014 r&p 001.22
[3] Amended effective 1/1/20, version 010 r&p 002.19

PART 2 ANALYSIS AND AUTHENTICATION[4]

2.1 Analysis and Authentication Types[5]

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:[6]

(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 authentication factors:[7]

(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). SCA *may be realised by various measures that use at least two authentication factors including, but not limited to, in-app push authorisation requests, text or email-supplied one-time passwords, or analysis of the data points within a transaction request if these data points provide at least two of the factors.* [8]

[4] Amended effective 1/1/20, version 010 r&p 002.19
[5] Amended effective 1/1/20, version 010 r&p 002.19
[6] Amended effective 1/1/20, version 010 r&p 002.19
[7] Inserted effective 1/1/24, version 017 r&p 003.23
[8] Last amended effective 1/1/24, version 017 r&p 003.23

2.1.3 *Fraud Controls*[9]

Fraud Controls are methods and practices that Acquirers, payment gateways and/or Merchants can implement to drive down fraud in CNP Transactions and include but are not limited to:

(a) One-time SMS or emails when a transaction exceeds a particular spend threshold to verify customers;

(b) Fraud systems designed to detect fraudulent transactions before a transaction is completed; and

(c) Actionable fraud alerts generated by merchant-issuer intelligence providing chargeback protection.

2.2 Exempt Transactions[10]

A transaction which is an Exempt Transaction for the purposes of SCA is any of the following:[11]

(a) Recurring Transaction, as set out in clause 2.2.1; [12]

(b) Trusted Customer Transaction, as set out in clause **Error! Reference source not found.**; or[13]

(c) Wallet Transaction, as set out in clause **Error! Reference source not found.**; [14]

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:[15]

(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;

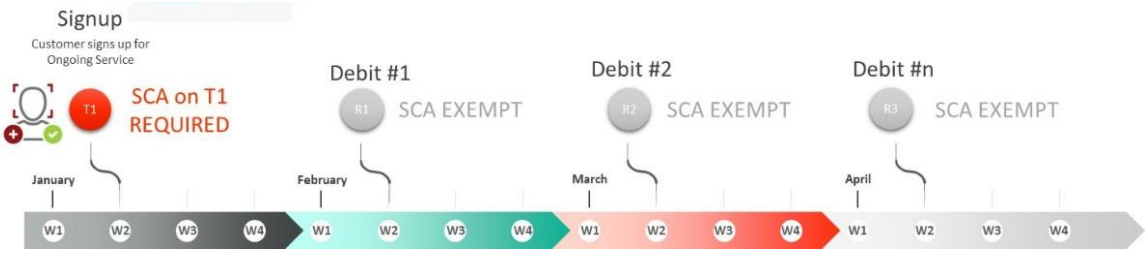
[9] Inserted effective 29/8/22, version 014 r&p 001.22
[10] Amended effective 1/1/20, version 010 r&p 002.19
[11] Amended effective 1/1/20, version 010 r&p 002.19
[12] Amended effective 1/1/20, version 010 r&p 002.19
[13] Amended effective 1/1/20, version 010 r&p 002.19
[14] Amended effective 1/1/20, version 010 r&p 002.19
[15] Amended effective 1/1/20, version 010 r&p 002.19

(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:[16]

(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.

[16] Amended effective 1/1/20, version 010 r&p 002.19

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:[17]

(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 [18]

(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 Part 3

[17] Amended effective 1/1/20, version 010 r&p 002.19
[18] Amended effective 1/1/20, version 010 r&p 002.19

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[19]

(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 3.1.4.

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.

3.1.2 *Issuer Fraud Rate and Threshold*[20]

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

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

[19] Amended effective 1/1/20, version 010 r&p 002.19

[20] Amended effective 1/1/20, version 010 r&p 002.19

Where:

(i) VALUE $_F$ in the Issuer Fraud Rate calculation is the total amount of that Issuer's settled, CNP Transactions that: [21]

(A) were Challenged CNP Transactions;

(B) had been passed through to the Issuer for SCA including Exempt Transactions;

(C) less any Out of Scope Transactions; and

(D) less any Challenged CNP Transactions that had been successfully defended by the Issuer, in the relevant Quarter for which the calculation is conducted.

Note: Challenged CNP Transactions are to be used in the calculation of Issuer Fraud Rate for the same Quarter as they are reported by the cardholder to the Issuer. If a Challenged CNP Transaction is successfully defended by the Issuer in a subsequent Quarter, the original Quarter's data may, at the Issuer's discretion, be resubmitted as provided in cl 3.1.3(c) below. A Challenged CNP Transaction which is successfully defended is a Challenged CNP Transaction where the Issuer provides evidence that the transaction was legitimate and does not refund the transaction to the cardholder. [22]

(ii) VALUE $_T$ 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, including any Exempt Transactions and less any Out of Scope Transactions, in the relevant Quarter for which the calculation is conducted.[23]

(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.

3.1.3 *Issuer Compliance*[24]

(a) Where an Issuer breaches the Issuer Fraud Threshold for one Quarter the Issuer should take measures to reduce their Issuer Fraud Rate. [25]

(b) Where an Issuer breaches the Issuer Fraud Threshold in two consecutive Quarters, that Issuer must perform SCA on all CNP Transactions that are passed through to the Issuer for SCA other than Exempt 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.[26]

[21] Amended effective 1/1/24, version 015 r&p 003.23
[22] Amended effective 1/1/24, version 015 r&p 003.23
[23] Amended effective 1/1/24, version 015 r&p 003.23
[24] Amended effective 1/1/20, version 010 r&p 002.19
[25] Inserted effective 29/8/22, version 014 r&p 001.22
[26] Last amended effective 1/1/24, version 015 r&p 003.23

(c) It is a Threshold Requirement that an Issuer not breach the Issuer Fraud Threshold for three consecutive Quarters.

3.1.4 *Issuer Reporting* [27]

(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).[28]

(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: [29]

(i) value of Challenged CNP Transactions that were passed through to the Issuer for SCA (irrespective of whether the Issuer performed requested SCA) less any Challenged CNP Transactions that were successfully defended in that Quarter; [30]

(ii) value of all CNP Transactions that were passed through to the Issuer for SCA [31]

(iii) value of CNP Transactions that were not passed through to the Issuer for SCA; [32]

(iv) value of all CNP Transactions that were not passed through to the Issuer for SCA;

(v) value of all Challenged CNP Transactions less any Challenged CNP Transactions that were passed through to the Issuer for SCA and successfully defended in that Quarter;[33]

(vi) value of all CNP Transactions; and

(vii) its Issuer Fraud Rate (bps).

(c) If, as a result of activities that occur after the end of a Quarter that impact transactions reported on in that Quarter's Issuer's Report, an Issuer no longer exceeds the Issuer Fraud Threshold in that Quarter: [34]

(i) within 90 days of the Reporting Date of that quarter the Issuer may inform AusPayNet in writing of the adjustment to the Issuer's Fraud Rate and resubmit its Issuer Report for that Quarter; and

(ii) if the Issuer resubmits its Issuer Report:

(A) AusPayNet will acknowledge receipt in writing within 14 days and confirm to the Issuer that the Issuer is no longer in breach

[27] Amended effective 1/1/20, version 010 r&p 002.19
[28] Amended effective 1/1/20, version 010 r&p 002.19
[29] Last amended effective 29/8/22, version 014 r&p 001.22
[30] Last amended effective 1/1/24, version 015 r&p 003.23
[31] amended effective 1/1/24, version 015 r&p 003.23
[32] amended effective 1/1/24, version 015 r&p 003.23
[33] amended effective 1/1/24, version 015 r&p 003.23
[34] Inserted effective 29/8/22, version 014 r&p 001.22

of the Issuer Fraud Threshold and is no longer required to take the measures to reduce its Issuer Fraud Rate previously advised; and

(B) if the Issuer has been advised of an imminent referral to the Sanctions Tribunal for breach of the Threshold Requirement, AusPayNet will confirm in writing that the process of referral to the Sanctions Tribunal is discontinued.

Note: If as a result of activities that occur after the end of a Quarter that impact transactions reported on in that Quarter's Issuer's Report, there is a substantial reduction in the amount by which the Issuer exceeds the Issuer Fraud Threshold in that Quarter, the Issuer:

(a) may inform the Company in writing; and

(b) whether or not the Issuer informs the Company, the Issuer may reference the reduction if the Issuer is ultimately referred to the Sanctions Tribunal for breach of the Threshold Requirement.

3.2 Obligations on Acquirers[35]

An Acquirer must:[36]

(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.

If a Merchant's ID changes but the Merchant remains under agreement with the same Acquirer to process and settle Card Payments:[37]

(i) the Merchant Fraud Rate shall be calculated in accordance with clause 3.2.2(a) for that Merchant with both Merchant IDs recorded;

(ii) where the Merchant exceeds the Merchant Fraud Threshold in any Quarter, the Acquirer must undertake the Acquirer Compliance obligations set out in Part 3.2.3; and

[35] Amended effective 1/1/20, version 010 r&p 002.19
[36] Amended effective 1/1/20, version 010 r&p 002.19
[37] Inserted effective 2/3/23, version 016 r&p 001.23

(iii) Quarters of breach of the Merchant Fraud Threshold by the Merchant will accrue consecutively, irrespective of the Merchant ID under which the Merchant was carrying on business.

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.

3.2.2 *Merchant Fraud Rate and Threshold*

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

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

Where:[38]

(i) VALUE_F 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_T 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_F 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_F of the Merchant Fraud Rate is $50,000 or higher.

[38] Amended effective 1/1/20, version 010 r&p 002.19

3.2.3 *Acquirer Compliance* [39]

(a) Where an Acquirer's Merchant exceeds the Merchant Fraud Threshold for one Quarter, that Acquirer must notify the Merchant:

(i) on or before the Reporting Date that the Merchant has exceeded the Merchant Fraud Threshold;

(ii) that the Merchant must implement Fraud Controls to reduce their Merchant Fraud Rate; and

(iii) that it is recommended ~~that~~ the Merchant perform SCA on a subset of CNP Transactions identified by the Merchant through a risk-based approach as high-risk transactions.

(b) Where an Acquirer's Merchant exceeds the Merchant Fraud Threshold for two consecutive Quarters, the Acquirer must notify the Merchant:

(i) on or before the Reporting Date that the Merchant has exceeded the Merchant Fraud Threshold:

(ii) that the Merchant must either require the Merchant to:

(C) perform SCA on all CNP Transactions excluding Exempt Transactions or;

(D) perform SCA on a subset of CNP Transactions, excluding Exempt Transactions, identified by the Merchant through a risk-based approach as high-risk transactions; or

(E) introduce additional Fraud Controls to those introduced in response to in the previous quarter's breach of the Merchant Fraud Threshold, or increase the sensitivity, reach or effectiveness of those Fraud Controls implemented in the previous Quarter.

(c) Where an Acquirer's Merchant exceeds the Merchant Fraud Threshold for three consecutive Quarters, the Acquirer must notify the Merchant:

(i) on or before the Reporting Date that the Merchant has exceeded the Merchant Fraud Threshold;

(ii) that the Merchant must pass all CNP Transactions excluding Exempt Transactions through to the Issuer for SCA until the Merchant's Fraud Rate for a Quarter no longer exceeds the Merchant Fraud Threshold;

(iii) that it is at the Issuer's discretion whether to perform SCA or Risk Based Analysis on transactions passed through by the Merchant.

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

[39] Last amended effective 29/8/22, version 014 r&p 001.22

3.2.4 *Acquirer Reporting* [40]

(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); [41]

(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).[42]

(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) (or where the Merchant changed its Merchant ID but remained under agreement with the same Acquirer, the Acquirer must record all Merchant IDs); [43]

(B) Merchant Category Code (MCC);

(C) Value of CNP Transactions;

(D) Value of Fraudulent CNP Transactions; and

(E) Merchant Fraud Rate calculation (bps).

(ii) The following information is required from those Acquirers who are in partnership with self-Acquirers. [44]

(A) All scheme-assigned aggregated Merchant Codes, per self-Acquirer; and[45]

(B) The information required at clause 3.2.3(b)(i), regardless of whether the self-Acquirer has exceeded the Merchant Fraud Threshold.[46]

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.

[40] Amended effective 1/1/20, version 010 r&p 002.19
[41] Amended effective 1/1/20, version 010 r&p 002.19
[42] Amended effective 1/1/20, version 010 r&p 002.19
[43] Amended effective 2/3/23, version 016 r&p 001.23
[44] Amended effective 1/1/20, version 010 r&p 002.19
[45] Amended effective 1/1/20, version 010 r&p 002.19
[46] Amended effective 1/1/20, version 010 r&p 002.19

(iii) An Acquirer Trend Report: For each of the following Merchant Fraud Rate categories:[47]

(C) <1 bps;

(D) 1 to <5 bps;

(E) 5 to <10 bps;

(F) 10 to <15 bps;

(G) 15 to <20 bps;

(H) 20 to <25 bps;

(I) 25 to <30 bps;

(J) 30 to <35 bps;

(K) 35 to <40 bps; and

(L) >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) volume (count) of Fraudulent CNP Transactions;

(O) volume (count) of all CNP Transactions;

(P) average Merchant Fraud Rate for that category.

Note:[48]

(i) Template reporting forms to be used by Acquirers in providing the above information is at clause 5.2 and 5.3.

(ii) 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;

[47] Amended effective 29/8/22, version 014 r&p 001.22
[48] Last amended effective 29/8/22, version 014 r&p 001.22

(ii) The information listed at clause 3.2.3(b)(i), using eftpos transaction data only.[49]

(d) If, as a result of activities that occur after the end of a Quarter that impact transactions reported on in the Quarter's Merchant Breach Report, the Merchant referenced in that Quarter's Merchant Breach Report no longer exceeds the Merchant Fraud Threshold in that Quarter:

(i) within 90 days of the Reporting Date of that quarter the Acquirer may inform AusPayNet in writing of the adjustment to the Merchant's Fraud Rate and resubmit its Merchant Breach Report for that Quarter; and

(ii) if the Acquirer resubmits its Merchant Breach Report:

(A) AusPayNet will acknowledge receipt in writing within 14 days and confirm to the Acquirer that the Merchant is no longer in breach and is no longer required to take the measures to reduce its Merchant Fraud Rate previously advised; and

(B) if the Acquirer has been advised of an imminent referral to the Sanctions Tribunal for breach of the Threshold Requirement, AusPayNet will confirm in writing that the process of referral to the Sanctions Tribunal is discontinued.

Note: If as a result of activities that occur after the end of a Quarter that impact transactions reported on in that Quarter's Merchant Breach Report, there is a substantial reduction in the amount by which the Acquirer's Merchant exceeds the Merchant Fraud Threshold in that Quarter, the Acquirer:

(a) may inform the Company in writing; and

(b) whether or not the Acquirer informs the Company, the Acquirer may reference the reduction if the Acquirer is ultimately referred to the Sanctions Tribunal for breach of the Threshold Requirement.

Next page is Part 4

[49] Amended effective 1/1/20, version 010 r&p 002.19

PART 4 THRESHOLD REQUIREMENTS AND SANCTIONS

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

Next page is Part 5.

PART 5 APPENDICES

5.1 Issuer Report Template

Report header: Issuer Name and ID, reporting period, USD-AUD exchange rate used (if required).[50]

Field ID	Field Name	Type	Value / Units	Field Definition
1	EcommAuthFraud	Numeric	AUD	Value of all Challenged settled, CNP Transactions that were passed through to the Issuer for SCA, (excluding MOTO) less any Challenged CNP Transactions that were successfully defended in that Quarter.
2	EcommAuthTotal	Numeric	AUD	Value of all settled, CNP Transactions that were passed through to the Issuer for SCA, (excluding MOTO)
3	EcommNoAuthFraud	Numeric	AUD	Value of all settled, Challenged CNP Transactions that were not passed through to the Issuer for SCA (excluding MOTO)
4	EcommNoAuthTotal	Numeric	AUD	Value of all settled, CNP Transactions that were not passed through to the Issuer for SCA (excluding MOTO)
5	EcommAllFraud	Numeric	AUD	Value of all settled, Challenged CNP Transactions, that were passed through to Issuer for SCA (excluding MOTO) less any Challenged CNP Transactions that were successfully defended in that Quarter.
6	EcommAllTotal	Numeric	AUD	Value of all (fraudulent + genuine) settled, CNP Transactions, (excluding MOTO)
9	IssuerFraudRate	Numeric	Basis points	Fraud Rate calculation: (Field #1 / Field #2) x10000

[50] Last amended effective 1/1/24, version 015 r&p 003.23

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

** Where the Merchant changed its Merchant ID but remained under agreement with the same Acquirer, all Merchant IDs are to be recorded for the Merchant).* [51]

5.2.1 *Acquirer Trend Report Template*

Report header: Acquirer name and ID, reporting period, USD-AUD exchange rate used (if required).[52]

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)
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)

[51] Amended effective 2/3/23, version 016 r&p 001.23
[52] Amended effective 29/8/22, version 014 r&p 001.22

11	AvgFraudRate	Numeric	Basis points	Fraud Rate calculation: (Field #3 / Field #4) 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