Effective:
1 July 2019
Version 009

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
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

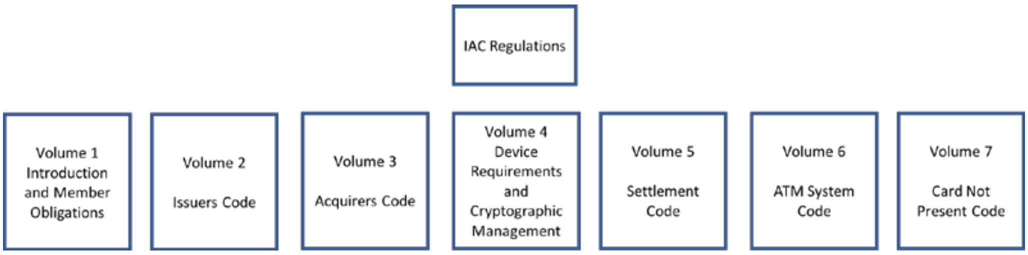
INDEX

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:


IAC Regulations
Volume 1 Introduction and Member Obligations
Volume 2 Issuers Code
Volume 3 Acquirers Code
Volume 4 Device Requirements and Cryptographic Management
Volume 5 Settlement Code
Volume 6 ATM System Code
Volume 7 Card Not Present Code

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 section 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.

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

(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 Australian.

1.4 Definitions

Definitions in Part 1, section 1.1 of the IAC Code Set Volume 1 are adopted in this Volume 7.

Authentication means SCA or Risk Based Analysis.

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.

Fraudulent CNP Transaction means a CNP Transaction which is also a Fraudulent Transaction.

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

(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.

Issuer Authentication means a Transaction in respect of which:

(a) the Issuer performs authentication; or

(b) Authentication by the Issuer is requested by a Merchant, Payment Gateway or Acquirer, irrespective of whether the Issuer performs the requested Authentication.

Issuer Fraud Rate means the aggregate of Fraudulent Transactions as calculated in accordance with section 3.1.2.

Issuer Fraud Threshold means the maximum allowable Issuer Fraud Rate as set out at section 3.1.2(d).

Merchant Fraud Rate means the aggregate of Fraudulent Transactions as calculated in accordance with section 3.4.1.

Merchant Fraud Threshold means the maximum allowable Merchant Fraud Rate as set at section 3.4.1(c).

Quarter means the unit of 3 months commencing on either 1 January, 1 April, 1 July or 1 September

Reporting Date means the 15th day of the month which follows the end of each Quarter, being 15 April, 15 July, 15 September 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.

Risk Based Analysis means Risk Based Analysis as defined in section 2.1.1.

SCA means SCA as defined in section 2.1.2.

Note: The following terms relevant to this Volume 7 are defined in Part 1, section 1.4 of Volume 1 of the IAC Code Set: Acquirer, Card, Cardholder, Issuer, Merchant, Threshold Requirement.

Next page is 2.1

PART 2 AUTHENTICATION

2.1 Division 1 – Authentication types

2.1.1 *Risk Based Analysis*

Risk Based Analysis is an authentication method that adapts the rigorousness of the identity verification and 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.

(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).

2.2 Division 2 – Exempt Transaction

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

(a) recurring transaction, as defined in section 2.2.2;

(b) trusted customer transaction, as defined in section 2.2.3; or

(c) wallet transaction, as defined in section 2.2.4;

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.

Note: all Exempt Transactions must be included in Fraud Rate calculations in sections 3.1.2 and 3.4.1.

2.2.2 *Recurring transaction*

"Recurring transaction" means 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:

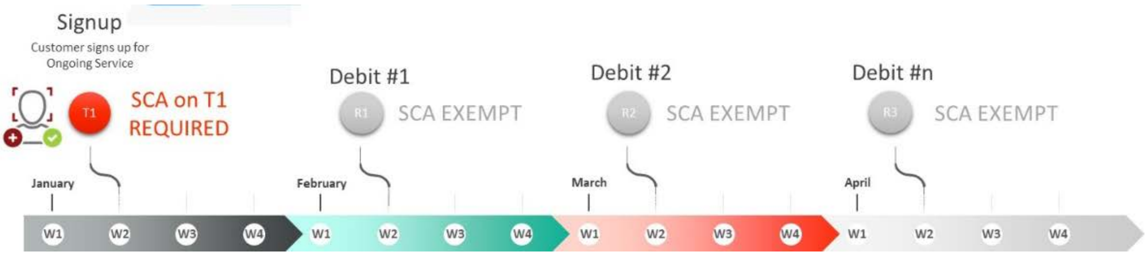
(a) acceptance of the Merchant's terms and conditions for that recurring series, which recurring series ends upon a change to those terms and conditions;

(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.



2.2.3 *Trusted customer transaction*

"Trusted customer transaction" means a subsequent CNP Transaction conducted by a customer with a Merchant, where:

(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:

(C) customer undertakes the subsequent transaction using the same device ID used by that customer in a previous transaction with the Merchant; or

(D) 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.

2.2.4 ***Wallet transactions***

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

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

(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 Division 1 – Obligations on Issuers

An Issuer must:

(a) calculate its Issuer Fraud Rate for the preceding Quarter in accordance with section 3.1.2.

(b) perform Authentication on a CNP Transaction upon receipt by the Issuer of a request for Authentication from a Merchant, Payment Gateway or Acquirer (the “requested transaction”), in the following way:

(i) if that Issuer’s Fraud Rate breached the Issuer Fraud Threshold for the preceding two consecutive Quarters, the Issuer must perform SCA on the requested transaction; and

(ii) for any Issuer to whom section 3.1(b)(i) does not apply, by performing either Risk Based Analysis or SCA on the requested transaction at the Issuer’s discretion;

except where the requested transaction is an Exempt Transaction.

(c) submit to AusPayNet any information required in section 3.3.

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*

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

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

(b) VALUE $_F$ in the Issuer Fraud Rate calculation is:

(i) the total amount of that Issuer's settled, Issuer Authenticated, Fraudulent CNP Transactions 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.

(c) VALUE $_T$ in the Issuer Fraud Rate calculation is the total amount of all of the Issuer's settled, Issuer Authenticated, CNP Transactions less any Out of Scope Transactions, in the relevant Quarter for which the calculation is conducted.

Breaching the Issuer Fraud Threshold

(d) The Issuer Fraud Threshold is set at an amount of less than 15 basis points.

(e) 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.

3.2 Division 2 – Issuer compliance and reporting

3.2.1 *Consecutive Quarters of breaching the Issuer Fraud Threshold*

(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 section 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.

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

3.3 Issuer reporting obligations

(a) On or before each Reporting Date, an Issuer is to provide to AusPayNet any information from the preceding Quarter required by section 3.3(b).

(b) An Issuer must provide, for each Quarter, the following information to AusPayNet in writing (in AUD where required):

(i) value of fraudulent Issuer Authenticated Fraudulent CNP Transactions;

(ii) value of all Issuer Authenticated CNP Transactions;

(iii) value of non-Issuer-Authenticated Fraudulent CNP Transactions;

(iv) value of all non-Issuer Authenticated CNP Transactions;

(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:

(i) A template reporting form to be used by Issuers in providing the above information is at section 5.1.

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

3.4 Division 3 – Acquirer obligations

3.4.1 *Merchant Fraud Rate and Threshold*

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

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

(b) Fraud Rate value inputs:

(i) VALUE $_F$ in the Merchant Fraud Rate calculation is the total amount of that Merchant’s settled, Fraudulent CNP Transactions less the value of any:

(A) Out of Scope Transactions; and

(B) Issuer Authenticated CNP 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 $_T$ in the Merchant Fraud Rate calculation is the total amount of that Merchant's settled, CNP Transactions less any Out of Scope Transactions, in the relevant Quarter for which the calculation is conducted.

Exceeding the Merchant Fraud Threshold

(c) The Merchant Fraud Threshold is set at:

(i) 20 basis points or higher; and

(ii) the amount in VALUE $_F$ of the Merchant Fraud Rate being $50,000 or higher.

(d) An Acquirer's Merchant exceeds the Merchant Fraud Threshold for any one Quarter, if:

(i) the Merchant Fraud Rate bps is 20 basis points or higher; and

(ii) the amount in VALUE $_F$ is $50,000 or higher.

An Acquirer must:

(a) calculate the Merchant Fraud Rate for the preceding Quarter for each of their Merchants (per Merchant ID) in accordance with section 3.4.1(a);

(b) if requested by their Merchant, notify that Merchant of their Merchant Fraud Rate for the preceding Quarter; and

(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 section 3.5; and

(e) submit to AusPayNet any information required in section 3.5.1(a).

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 fraud rates, regardless of request or exceeding the Merchant Fraud Threshold.

3.5 Division 4 – Acquirer compliance reporting

Consecutive Quarters of an Acquirer's Merchant exceeding the Merchant Fraud Threshold:

(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 Quarters, it is recommended (but not required) that the Merchant pass all CNP Transactions through to the Issuer for Issuer Authentication.

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

3.5.1 *Acquirer reporting obligations*

(a) On or before each Reporting Date:

(i) an Acquirer is to provide to AusPayNet any information from the preceding Quarter required by section 3.5.1(b);

(ii) a self-Acquirer is to provide to AusPayNet any information from the preceding Quarter required by section 3.5.1(b) and 3.5.1(c).

(b) An Acquirer must, for each Quarter, provide the following information to AusPayNet in writing (in AUD where required):

(i) <u>Merchant Breach Report:</u> 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 Catgegory Code (MCC);

(C) Value of CNP Transactions;

(D) Value of Fraudulent CNP Transactions; and

(E) Merchant Fraud Rate calculation (bps).

(ii) Self Acquirers Report: The following information for self-Acquirers only:

(A) All scheme-assigned aggregated Merchant Codes, per Acquirer;

(B) The information required at section 3.5.1(b)(i), regardless of whether the merchant has exceeded the Merchant Fraud Threshold;

(C) The information listed at section 3.5.1(b)(i), using eftpos transaction data only.

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) <u>An Acquirer Trend Report:</u> 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:

(i) Reporting at sections 3.10(b)(iii)(L) to 3.10(b)(iii)(Q) excludes MOTO as it is an Out of Scope Transaction.

(ii) Template reporting forms to be used by Acquirers in providing the above information is at section 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 section 3.10(b)(i), regardless of whether the Merchant has exceeded the Merchant Fraud Threshold; and

(iii) The information listed at section 3.10(b)(i), using eftpos transaction data only.

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 authentication (excluding MOTO)
2	EcommAuthTotal	Numeric	AUD	Value of all (fraudulent + genuine) settled, CNP Transactions that were passed through to the Issuer for authentication (excluding MOTO)
3	EcommNoAuthFraud	Numeric	AUD	Value of all fraudulent settled, CNP Transactions that were not passed through to the Issuer for authentication (excluding MOTO)
4	EcommNoAuthTotal	Numeric	AUD	Value of all (fraudulent + genuine) settled, CNP Transactions that were not passed through to the Issuer for authentication (excluding MOTO)
5	EcommAllFraud	Numeric	AUD	Value of all fraudulent settled, CNP Transactions, regardless of whether passed through to Issuer for authentication (excluding MOTO)
6	EcommAllTotal	Numeric	AUD	Value of all (fraudulent + genuine) settled, CNP Transactions, regardless of whether passed through to Issuer for authentication (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