Form A

Commonwealth of Australia

Competition and Consumer Act 2010 — subsections 88 (1A) and (1)

EXCLUSIONARY PROVISIONS AND ASSOCIATED CARTEL PROVISIONS: APPLICATION FOR AUTHORISATION

To the Australian Competition and Consumer Commission:
Application is hereby made under subsection(s) 88 (1A)/88 (1) of the *Competition and Consumer Act 2010* for an authorisation:

- to make a contract or arrangement, or arrive at an understanding, a provision of which would be, or might be, a cartel provision within the meaning of Division 1 of Part IV of that Act and which would also be, or might also be, an exclusionary provision within the meaning of section 45 of that Act.

- to give effect to a provision of a contract, arrangement or understanding that is, or may be, a cartel provision within the meaning of Division 1 of Part IV of that Act and which is also, or may also be, an exclusionary provision within the meaning of section 45 of that Act.

- to make a contract or arrangement, or arrive at an understanding, where a provision of the proposed contract, arrangement or understanding would be, or might be, an exclusionary provision within the meaning of section 45 of that Act.

- to give effect to a provision of a contract, arrangement or understanding where the provision is, or may be, an exclusionary provision within the meaning of section 45 of that Act.

PLEASE FOLLOW DIRECTIONS ON BACK OF THIS FORM

1. Applicant

(a) Name of Applicant:

A91525 Australian Payments Clearing Association Limited (ABN 12 055 136 519).

(b) Description of business carried on by applicant:

Coordination and management of the implementation, operation and development of effective clearing systems, including industry initiatives and projects in the card payments industry.

(c) Address in Australia for service of documents on the applicant:

c/- Rowan McMonnies

Partner

Baker & McKenzie

Level 27, 50 Bridge Street

Sydney NSW 2000

2. Contract, arrangement or understanding

(a) Description of the contract, arrangement or understanding, whether proposed or actual, for which authorisation is sought:

See 2(b) below.

(b) Description of those provisions of the contract, arrangement or understanding described at 2 (a) that are, or would or might be, exclusionary provisions and (if applicable) are, or would or might be, cartel provisions:

The conduct for which authorisation is sought involves APCA and those card schemes, issuers and acquirers that form the current and prospective IAC members agreeing to:

i) make changes to the IAC Regulations and Code Set and/or the credit, debit and charge card scheme rules for the sole purpose of implementing 3D Secure security measures to provide for:

- the mandatory enrolment in the 3D Secure security measures of both all relevant payment cards issued in Australia and all online merchants in Australia;
- the determination of fraud risk thresholds that are focused on targeting high risk online transactions to determine when 3D Secure should be applied to an online transaction and when such an online transaction should be challenged by the use of dynamic authentication measures; and
- the application of 3D Secure security measures based on fraud risk thresholds to particular online transactions involving particular Australian based merchants in which credit, debit or charge card numbers are entered on the merchant's website;

ii) implement the measures in (a) in a common timeframe; and

iii) jointly fund and implement a public communications strategy in relation to the proposed arrangements in (a) and (b),

together, the **3D Secure arrangements**.

The Applicant does not concede that the 3D Secure arrangements do or would contravene the Competition and Consumer Act 2010 (Cth).

There is nothing in the 3D secure arrangements that would preclude the Applicants and IAC members from competing beyond the scope of the 3D secure arrangements in relation to card transaction security measures or any other aspect of card payments.

(c) Description of the goods or services to which the contract, arrangement or understanding (whether proposed or actual) relate:

Online transactions.

(d) The term for which authorisation of the provision of the contract, arrangement or understanding (whether proposed or actual) is being sought and grounds supporting this period of authorisation:

5 years.

3. Parties to the proposed arrangement

(a) Names, addresses and descriptions of business carried on by other parties or proposed parties to the contract or proposed contract, arrangement or understanding:

The 3D secure arrangements will be entered into and given effect to by the Applicant and IAC members or some of them.

Refer to Attachment A of the Supporting Submission for details of IAC members at the date of this application.

(b) Names, addresses and descriptions of business carried on by parties and other persons on whose behalf this application is made:

Persons who may become IAC members after the date of this application.

4. Public benefit claims

(a) Arguments in support of application for authorisation:

Refer to the Supporting Submission.

(b) Facts and evidence relied upon in support of these claims:

Refer to the Supporting Submission.

5. Market definition

Provide a description of the market(s) in which the goods or services described at 2 (c) are supplied or acquired and other affected markets including: significant suppliers and acquirers; substitutes available for the relevant goods or services; any restriction on the supply or acquisition of the relevant goods or services (for example geographic or legal restrictions):

Refer to the Supporting Submission.

6. Public detriments

(a) Detriments to the public resulting or likely to result from the contract arrangement or understanding for which authorisation is sought, in particular the likely effect of the contract arrangement or understanding, on the prices of the goods or services described at 2 (c) and the prices of goods or services in other affected markets:

Refer to the Supporting Submission.

(b) Facts and evidence relevant to these detriments:

Refer to the Supporting Submission.

7. Contracts, arrangements or understandings in similar terms

(a) This application for authorisation may also be expressed to be made in relation to other contracts, arrangements or understandings or proposed contracts, arrangements or understandings, that are or will be in similar terms to the abovementioned contract, arrangement or understanding:

(b) Is this application to be so expressed?

This application is made in relation to all parties and potential parties to a contract arrangement or understanding constituted by the 3D secure arrangements.

(c) If so, the following information is to be furnished:

(i) description of any variations between the contract, arrangement or understanding for which authorisation is sought and those contracts, arrangements or understandings that are stated to be in similar terms:

Not applicable.

(ii) Where the parties to the similar term contract(s) are known — names, addresses and descriptions of business carried on by those other parties:

Refer to Attachment A of the Supporting Submission for details of IAC members at the date of this application.

(iii) Where the parties to the similar term contract(s) are not known — description of the class of business carried on by those possible parties:

Not applicable.

8. Joint Ventures

(a) Does this application deal with a matter relating to a joint venture (See section 4J of the *Competition and Consumer Act 2010*)?

Yes

(b) If so, are any other applications being made simultaneously with this application in relation to that joint venture?

Not applicable.

(c) If so, by whom or on whose behalf are those other applications being made?

Not applicable.

9. Further information

(a) Name, postal address and telephone contact details of the person authorised by the applicant seeking authorisation to provide additional information in relation to this application:

c/- Rowan McMonnies

Partner

Baker & McKenzie

Level 27, 50 Bridge Street

Sydney NSW 2000

Dated 28 January 2016

Signed by/on behalf of the applicant

R.C. McMonnies

.....

Rowan McMonnies
Partner
Baker & McKenzie

DIRECTIONS

1. Use Form A if the contract, arrangement or understanding includes a provision which is, or might be, a cartel provision and which is also, or might also be, an exclusionary provision. Use Form B if the contract, arrangement or understanding includes a provision which is, or might be, a cartel provision or a provision which would have the purpose, or would or might have the effect, of substantially lessening competition. It may be necessary to use both forms for the same contract, arrangement or understanding.

   In lodging this form, applicants must include all information, including supporting evidence, that they wish the Commission to take into account in assessing their application for authorisation.

   Where there is insufficient space on this form to furnish the required information, the information is to be shown on separate sheets, numbered consecutively and signed by or on behalf of the applicant.

2. Where the application is made by or on behalf of a corporation, the name of the corporation is to be inserted in item 1 (a), not the name of the person signing the application and the application is to be signed by a person authorised by the corporation to do so.

3. Describe that part of the applicant's business relating to the subject matter of the contract, arrangement or understanding in respect of which authorisation is sought.

4. Provide details of the contract, arrangement or understanding (whether proposed or actual) in respect of which the authorisation is sought. Provide details of those provisions of the contract, arrangement or understanding that are, or would or might be, exclusionary provisions. Provide details of those provisions of the contract, arrangement or understanding that are, or would or might be, cartel provisions.

   In providing these details:

   (a) to the extent that any of the details have been reduced to writing, provide a true copy of the writing; and

   (b) to the extent that any of the details have not been reduced to writing, provide a full and correct description of the particulars that have not been reduced to writing.

5. Where authorisation is sought on behalf of other parties provide details of each of those parties including names, addresses, descriptions of the business activities engaged in relating to the subject matter of the authorisation, and evidence of the party's consent to authorisation being sought on their behalf.

6. Provide details of those public benefits claimed to result or to be likely to result from the proposed contract, arrangement or understanding including quantification of those benefits where possible.

7. Provide details of the market(s) likely to be effected by the contract, arrangement or understanding in particular having regard to goods or services that may be substitutes for the good or service that is the subject matter of the application for authorisation.

8. Provide details of the detriments to the public, including those resulting from any lessening of competition, which may result from the proposed contract, arrangement or understanding. Provide quantification of those detriments where possible.

9. Where the application is made also in respect of other contracts, arrangements or understandings, which are or will be in similar terms to the contract, arrangement or understanding referred to in item 2, furnish with the application details of the manner in which those contracts, arrangements or understandings vary in their terms from the contract, arrangements or understanding referred to in item 2.

10. Where authorisation is sought on behalf of other parties provide details of each of those parties including names, addresses, and descriptions of the business activities engaged in relating to the subject matter of the authorisation, and evidence of the party's consent to authorisation being sought on their behalf.

Form B

Commonwealth of Australia

Competition and Consumer Act 2010 — subsections 88 (1A) and (1)

AGREEMENTS AFFECTING COMPETITION OR INCORPORATING RELATED CARTEL PROVISIONS: APPLICATION FOR AUTHORISATION

To the Australian Competition and Consumer Commission:
Application is hereby made under subsection(s) 88 (1A)/88 (1) of the *Competition and Consumer Act 2010* for an authorisation:

- to make a contract or arrangement, or arrive at an understanding, a provision of which would be, or might be, a cartel provision within the meaning of Division 1 of Part IV of that Act (other than a provision which would also be, or might also be, an exclusionary provision within the meaning of section 45 of that Act).

- to give effect to a provision of a contract, arrangement or understanding that is, or may be, a cartel provision within the meaning of Division 1 of Part IV of that Act (other than a provision which is also, or may also be, an exclusionary provision within the meaning of section 45 of that Act).

- to make a contract or arrangement, or arrive at an understanding, a provision of which would have the purpose, or would or might have the effect, of substantially lessening competition within the meaning of section 45 of that Act.

- to give effect to a provision of a contract, arrangement or understanding which provision has the purpose, or has or may have the effect, of substantially lessening competition within the meaning of section 45 of that Act.

PLEASE FOLLOW DIRECTIONS ON BACK OF THIS FORM

1. Applicant

(a) Name of Applicant:

A91526 Australian Payments Clearing Association Limited (ABN 12 055 136 519).

(b) Short description of business carried on by applicant:

Coordination and management of the implementation, operation and development of effective clearing systems, including fraud protection industry initiatives in the card payments industry.

(c) Address in Australia for service of documents on the applicant:

c/- Rowan McMonnies

Partner

Baker & McKenzie

Level 27, 50 Bridge Street

Sydney NSW 2000

2. Contract, arrangement or understanding

(a) Description of the contract, arrangement or understanding, whether proposed or actual, for which authorisation is sought:
(Refer to direction 4)

See 2(b) below.

(b) Description of those provisions of the contract, arrangement or understanding described at 2 (a) that are, or would or might be, cartel provisions, or that do, or would or might, have the effect of substantially lessening competition:
(Refer to direction 4)

The conduct for which authorisation is sought involves APCA and those card schemes, issuers and acquirers that form the current and prospective IAC members agreeing to:

i) make changes to the IAC Regulations and Code Set and/or the credit, debit and charge card scheme rules for the sole purpose of implementing 3D Secure security measures to provide for:

- the mandatory enrolment in the 3D Secure security measures of both all relevant payment cards issued in Australia and all online merchants in Australia;
- the determination of fraud risk thresholds that are focused on targeting high risk online transactions to determine when 3D Secure should be applied to an online transaction and when such an online transaction should be challenged by the use of dynamic authentication measures; and
- the application of 3D Secure security measures based on fraud risk thresholds to particular online transactions involving particular Australian based merchants in which credit, debit or charge card numbers are entered on the merchant's website;

ii) implement the measures in (a) in a common timeframe; and

iii) jointly fund and implement a public communications strategy in relation to the proposed arrangements in (a) and (b),

together, the **3D Secure arrangements**.

The Applicant does not concede that the 3D secure arrangements do or would contravene the Competition and Consumer Act 2010 (Cth).

There is nothing in the 3D secure arrangements that would preclude the Applicants and IAC members from competing beyond the scope of the 3D secure arrangements in relation to card transaction security measures or any other aspect of card payments.

(c) Description of the goods or services to which the contract, arrangement or understanding (whether proposed or actual) relate:

Online transactions.

(d) The term for which authorisation of the contract, arrangement or understanding (whether proposed or actual) is being sought and grounds supporting this period of authorisation:

5 years.

3. Parties to the proposed arrangement

(a) Names, addresses and descriptions of business carried on by other parties or proposed parties to the contract or proposed contract, arrangement or understanding:

The 3D secure arrangements will be entered into and given effect to by the Applicant and IAC members or some of them.

Refer to Attachment A of the Supporting Submission for details of IAC members at the date of this application .

(b) Names, addresses and descriptions of business carried on by parties and other persons on whose behalf this application is made:
(Refer to direction 5)

Persons who may become IAC members after the date of this application.

4. Public benefit claims

(a) Arguments in support of authorisation:

Refer to the Supporting Submission.

(b) Facts and evidence relied upon in support of these claims:

Refer to the Supporting Submission.

5. Market definition

Provide a description of the market(s) in which the goods or services described at 2 (c) are supplied or acquired and other affected markets including: significant suppliers and acquirers; substitutes available for the relevant goods or services; any restriction on the supply or acquisition of the relevant goods or services (for example geographic or legal restrictions):

Refer to the Supporting Submission.

6. Public detriments

(a) Detriments to the public resulting or likely to result from the authorisation, in particular the likely effect of the contract, arrangement or understanding, on the prices of the goods or services described at 2 (c) and the prices of goods or services in other affected markets:

Refer to the Supporting Submission.

(b) Facts and evidence relevant to these detriments:

Refer to the Supporting Submission.

7. Contract, arrangements or understandings in similar terms

This application for authorisation may also be expressed to be made in relation to other contracts, arrangements or understandings or proposed contracts, arrangements or understandings, that are or will be in similar terms to the abovementioned contract, arrangement or understanding.

(a) Is this application to be so expressed?

This application is made in relation to all parties and potential parties to a contract arrangement or understanding constituted by the 3D secure arrangements.

(b) If so, the following information is to be furnished:

(i) description of any variations between the contract, arrangement or understanding for which authorisation is sought and those contracts, arrangements or understandings that are stated to be in similar terms:
(Refer to direction 9)

Not applicable.

(ii) Where the parties to the similar term contract(s) are known — names, addresses and descriptions of business carried on by those other parties:

Refer to Attachment A of the Supporting Submission for details of IAC members at the date of this application.

(iii) Where the parties to the similar term contract(s) are not known — description of the class of business carried on by those possible parties:

Not applicable.

8. Joint Ventures

(a) Does this application deal with a matter relating to a joint venture (See section 4J of the *Competition and Consumer Act 2010*)?

Yes.

(b) If so, are any other applications being made simultaneously with this application in relation to that joint venture?

Not applicable.

(c) If so, by whom or on whose behalf are those other applications being made?

Not applicable.

9. Further information

(a) Name and address of person authorised by the applicant to provide additional information in relation to this application:

c/- Rowan McMonnies

Partner

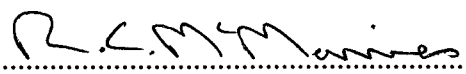
Baker & McKenzie

Level 27, 50 Bridge Street

Sydney NSW 2000

Dated 28 January 2016

Signed by/on behalf of the applicant



Rowan McMonnies
Partner
Baker & McKenzie

DIRECTIONS

1. Use Form A if the contract, arrangement or understanding includes a provision which is, or might be, a cartel provision and which is also, or might also be, an exclusionary provision. Use Form B if the contract, arrangement or understanding includes a provision which is, or might be, a cartel provision or a provision which would have the purpose, or would or might have the effect, of substantially lessening competition. It may be necessary to use both forms for the same contract, arrangement or understanding.

   In lodging this form, applicants must include all information, including supporting evidence, that they wish the Commission to take into account in assessing the application for authorisation.

   Where there is insufficient space on this form to furnish the required information, the information is to be shown on separate sheets, numbered consecutively and signed by or on behalf of the applicant.

2. Where the application is made by or on behalf of a corporation, the name of the corporation is to be inserted in item 1 (a), not the name of the person signing the application and the application is to be signed by a person authorised by the corporation to do so.

3. Describe that part of the applicant's business relating to the subject matter of the contract, arrangement or understanding in respect of which the application is made.

4. Provide details of the contract, arrangement or understanding (whether proposed or actual) in respect of which the authorisation is sought. Provide details of those provisions of the contract, arrangement or understanding that are, or would or might be, cartel provisions. Provide details of those provisions of the contract, arrangement or understanding that do, or would or might, substantially lessen competition.

   In providing these details:

   (a) to the extent that any of the details have been reduced to writing, provide a true copy of the writing; and

   (b) to the extent that any of the details have not been reduced to writing, provide a full and correct description of the particulars that have not been reduced to writing.

5. Where authorisation is sought on behalf of other parties provide details of each of those parties including names, addresses, descriptions of the business activities engaged in relating to the subject matter of the authorisation, and evidence of the party's consent to authorisation being sought on their behalf.

6. Provide details of those public benefits claimed to result or to be likely to result from the proposed contract, arrangement or understanding including quantification of those benefits where possible.

7. Provide details of the market(s) likely to be effected by the contract, arrangement or understanding, in particular having regard to goods or services that may be substitutes for the good or service that is the subject matter of the authorisation.

8. Provide details of the detriments to the public which may result from the proposed contract, arrangement or understanding including quantification of those detriments where possible.

9. Where the application is made also in respect of other contracts, arrangements or understandings, which are or will be in similar terms to the contract, arrangement or understanding referred to in item 2, furnish with the application details of the manner in which those contracts, arrangements or understandings vary in their terms from the contract, arrangements or understanding referred to in item 2.

Australian Payments Clearing Association

SUBMISSION TO THE AUSTRALIAN COMPETITION AND CONSUMER COMMISSION IN SUPPORT OF THE APPLICATION FOR AUTHORISATION AND INTERIM AUTHORISATION

AUSTRALIAN PAYMENTS CLEARING ASSOCIATION LIMITED

JANUARY 2016

TABLE OF CONTENTS

1. INTRODUCTION

The Australian Payments Clearing Association Limited (APCA) has requested authorisation and interim authorisation for the proposed implementation of an industry wide transaction security initiative to mitigate online payments transaction fraud.

This submission sets out the context in which the application has been made and the details to support the following basis for authorisation and interim authorisation being granted:

a) online payments transaction fraud is a cost and concern to consumers and has increased significantly in recent years. Consumers are impacted by online payments transaction fraud in four important ways:

   i) consumers meet the cost of fraud through increases in the price of goods purchased online and the cost of payments services;

   ii) consumers are inconvenienced by fraud through meeting the cost of fraudulent transactions that they do not identify, the need to request the reversal of fraudulent transactions, obtain new cards, re-establish direct debits on the new card account;

   iii) consumers experience undermined confidence in the online payments system and the loss of efficiencies through utilising online payments, the expansion of which is a policy of the Australian Federal Government; and

   iv) consumers face significant risks associated with fraud through the disclosure of personal information and potentially identity theft,

b) despite concerted effort, the payments industry has been unable to arrive at an effective solution to address online payment transaction fraud (having previously achieved PIN@POS in the physical shopping environment);

c) the coordination provided for in this application for authorisation is necessary to facilitate an effective industry-wide response to online payments transaction fraud;

d) significant net public benefits will arise from the authorised conduct including clear net benefits to consumers; and

e) in order to ensure those benefits can be realised in a timely way, an interim authorisation is requested to provide for preparatory steps to be undertaken as soon as possible.

In addition, this submission sets out the importance of interim authorisation being granted from the date of the ACCC draft determination to facilitate preparatory steps required to implement the authorised conduct. These preparatory steps involve:

a) making the necessary card scheme changes to provide for the proposed conduct;

b) issuers, acquirers and an initial tranche of Australian online merchants that experience significantly above average fraud levels taking steps to prepare for the implementation of the proposed conduct as soon as possible in 2017; and

c) commencing the development of a broad communications strategy to support the implementation of the proposed conduct.

In the context of the nature and scope of the proposed conduct and the preparatory steps required and the implications of delayed implementation of the proposed conduct (e.g. approximately $10 million of fraud losses suffered by Australian online merchants for each month of delay), the criteria for an interim authorisation are satisfied and the benefits of the proposed conduct to consumers and the industry should not be unnecessarily delayed.

2. BACKGROUND

2.1 APCA

APCA is the primary industry vehicle for payments industry collaboration in Australia. APCA was established in 1992 to manage and develop regulations, procedures, policies and standards governing payments clearing and settlement within Australia. Historically, its focus has been on the administration of a number of clearing systems, notably the systems for cheques, 'direct entry' (bulk electronic payments), aspects of ATM/EFTPOS/card transactions, high value transactions and wholesale cash.

These systems are critical for the secure and efficient operation of the Australian payments system by providing shared self-regulatory rules and procedures for system members. APCA supports these systems through providing secretariat, compliance and other support to member governance groups. In Australia, institutions involved in the payments system have historically exchanged payment messages bilaterally.

As part of its role, APCA maintains device security standards and a number of key industry databases which support the efficient operation of Australian payments. APCA also collects payments statistics that inform member decision-making and provide critical information for stakeholders. This includes information about payment system volumes and values, the number of ATMs and EFTPOS devices in Australia and fraud statistics.

APCA provides information to the community about payments through the APCA website, publications and education campaigns. APCA engages with stakeholders bilaterally as well as through APCA-supported initiatives such as the APCA Stakeholder Forum.

APCA has also worked towards a strategic agenda for Australian payments. This has been through the publication of Low Value Payments: An Australian Roadmap (the LVP Roadmap), policy submissions and discussion papers on issues such as the future of cheques, future of cash, online payments and industry co- regulation. APCA has supported the implementation of new innovation in payments through its industry projects, such as an enhanced communication network known as the Community of Interest Network (or COIN infrastructure network), and by providing thought leadership and opportunities for discussion about innovation within the industry, in particular through the New Payments Platform and the Australian Payments Council, as well as coordinating the industry implementation of Direct Entry Same Day Settlement.

In recent years, APCA has reformed its governance, opening up membership as well as opportunities to participate in APCA decision-making. This has resulted in APCA

appointing three voting independent directors and the expansion of APCA membership beyond clearing system members to a wider range of payment organisations.

To facilitate these reforms APCA recently introduced a new Issuers and Acquirers Community (**IAC**) framework to replace the Consumer Electronic Clearing System framework. The IAC, which is managed by the Issuers and Acquirers Forum (**IAF**) has a broader remit than the CECS framework and the ability to admit a broader range of entities as members, including:

a) Issuer and Acquirer Participants, being the financial institutions that issue and acquire credit, debit and charge cards and card payments in Australia; and

b) Operator Members and Affiliates, being the organisations that participate in the Australian payments market but are not responsible for transaction volume, such as the domestic and global payment card schemes.

The IAC operates in accordance with the IAC Regulations and the IAC Code Set which, after a transition period, will replace the CECS rules.

The purpose of establishing the IAC was to facilitate industry engagement in card payments industry policy development, including a stronger focus on monitoring and managing compliance with security standards and requirements. The arrangements facilitating the establishment of the IAC were the subject of an application to the ACCC for authorisation, with authorisation granted in August 2015.

2.2 Card not present fraud

The Australian payments market is characterised by a clear long term trend away from cash to electronic payment methods, such as credit, debit and charge cards. This has been driven in part by the increasing importance of online commerce, which provides convenience and efficiency benefits to both merchants and consumers. The remote and 'always on' nature on online commerce is attractive to merchants and consumers alike. For merchants, it enables:

a) a massive geographic reach without having to invest in multiple physical points of presence (both lowering costs and increasing the size of the available market);

b) sales to occur 24 x 7; and

c) small merchants to compete like they were large merchants.

For consumers, it enables:

a) the ability to comparison shop across a vast array of offers, both domestic and overseas;

b) purchases to occur 24 x 7; and

c) the convenience of shopping from the home / the office / anywhere.

Hence the ever increasing importance of the internet has meant a burgeoning online economy with online payments growing alongside it. Globally households are directing a greater portion of their payments online, whether for shopping for the latest iPhone, booking a holiday or paying their utility bills. Indeed, global online sales are reported to have reached USD$1.5 trillion in 2014, an increase of 20.1 per cent over the prior year, and with forecasts of USD$2.0 trillion in 2016 (The eMarketer http://www.emarketer.com).

Indeed, Reserve Bank of Australia (**RBA**) payments data demonstrates that online payments have more than doubled since 2007 to now represent 45 per cent of all transactions (RBA Payments Diary 2014).

Many jurisdictions have attacked fraud at the physical point of sale by instituting Chip&PIN (or PIN@POS) on card payments, the fraudsters have moved their attention to the online environment where the entry of card details to make a purchase has been historically less secure. This movement of criminal attention has occurred at the same time as the importance of online commerce to most economies has increased. In dollar terms, gross fraud losses on Australian issued cards used in a card not present environment totalled $300 million in 2014, which was a 40 per cent increase on the previous year (*Australian Payments Fraud - Details and data 2015*). This trend is forecast to continue with an increasing number and value of transactions being completed online and increased criminal attention to this channel.

The vast majority of online transactions involve the use of a card of the international payment schemes (Visa, MasterCard and American Express), with BPAY and PayPal being large but secondary payment methods. As a result, the vast majority of online transactions involve cardholders across Australia being required to enter a credit, debit or charge card number, the expiry date and the card verification value code (CVC) into a merchant website on a computer or other device.

Online transactions inherently involve the card not being physically available for the merchant to inspect at the time of the transaction, referred to as a 'card not present' transaction (**CNP transaction**). CNP transactions include online transactions and mail order or telephone transactions, but with the vast majority being online transactions. Online transactions are primarily carried out by either a cardholder entering their payment card number into the merchant website, the merchant keeping the cardholder’s details on file from a previous transaction or through the use of a digital wallet (such as PayPal).

CNP transactions provide increased scope for fraud, as there is greater potential for the transaction to be facilitated by someone other than the cardholder. As a result, the significant increase in e-commerce and online transactions has corresponded with a substantial increase in payments fraud.

Payments fraud in the context of a CNP transaction (**CNPF**) can arise in a number of contexts including through cardholder information being:

a) obtained illegally through card theft, malware on the cardholder's device or merchant database hacking;

b) intercepted through communications systems; or

c) obtained by cardholder deception such as through 'phishing' scams, in which fake communications (i.e. emails) that purport to come from a genuine source are used to encourage cardholders to provide information.

Fraud statistics published by APCA (*Australian Payments Fraud - Details and data 2015*) indicate that in 2014:

a) fraud on Australian payment cards increased from 46.6 cents to 58.8 cents in every $1,000 spent; and

b) CNPF made up 77 per cent of all payments card fraud in Australia by value.

A factor contributing to the growth in CNPF has been successful security initiatives in relation to card present transactions, including the introduction of chip cards (which are almost impossible to duplicate) and mandatory use of PIN authentication (which reduced lost and stolen card fraud). These increased security measures have made CNPF relatively easier for criminals to engage in than at physical point of sale.

Online payments fraud is an issue of concern both across the payments industry as well as for consumers. Consumers are impacted by online payments transaction fraud in four important ways:

a) consumers meet the cost of fraud through increases in the price of goods purchased online and the cost of payments services;

b) consumers are inconvenienced by fraud through meeting the cost of fraudulent transactions that they do not identify, the need to request the reversal of fraudulent transactions, obtain new cards, re-establish direct debits on the new card account;

c) consumers experience undermined confidence in the online payments system and the loss of efficiencies through utilising online payments, the expansion of which is a policy of the Australian Federal Government; and

d) consumers face significant risks associated with fraud through the disclosure of personal information and potentially identity theft.

In this context, an online survey completed by RFI Consulting in 2012 found that although consumers were very comfortable with online purchasing, 38 per cent of survey respondents said they were still very concerned about the security of their personal information online.

2.3 CNPF project

In response to increasing concern regarding the rate of growth of CNPF the IAC established the CNPF project managed by the IAC CNPF Working Group. The CNPF Working Group has been exploring the available options to address, reduce and mitigate CNPF, and the extent to which the options would require an industry-wide solution. This work, which involved the advice of expert consultants, identified a range of options available to address CNPF which may be used separately or in combination, including:

a) data analytics, which seek to identify suspicious transactions or devices and flag or stop the relevant transaction from being completed;

b) tokenisation, in which the cardholder information in a merchant database is converted into a form in which it cannot be used for CNPF;

c) biometrics, for example voice recognition in which a cardholder seeking to complete a transaction that has been flagged as potentially suspicious is required to provide a 'voiceprint' in response to an issuer system telephone call;

d) authentication processes such as security token or SMS/text message which involve passwords to be used by cardholders to complete transactions. This is referred to as a 2-factor cardholder authentication process, in that the cardholder requires both information from the card and the password (separate to the card) to complete the transaction; and

e) 3D Secure which involves a protocol (set of rules) to identify a potentially fraudulent card transaction and provide for authentication of the cardholder through the provision of a password based challenge. 3D Secure is based on a three domain model in which information is exchanged between the acquirer domain, being the merchant and the bank to which money is being paid, the issuer domain, being the bank who issued the card being used and the interoperability domain, being the infrastructure provided by the payment card scheme to support the 3D Secure protocol. The process steps involved in a 3D Secure transaction include:

   i) the merchant or payment gateway that is contracted by the merchant routing the transaction through to an access control server (**ACS**) service provider, that is contracted to/by the card issuer to apply fraud risk analytics;

   ii) the ACS service provider processing the transaction using the available data on the transaction, the cardholder, the cardholder's past transaction behaviour and a rule set to determine the level of risk;

   iii) the issuer determining whether or not to challenge the transaction based on the level of risk identified. The issuer may also determine to accept or decline the transaction without initiating a challenge;

   iv) if the issuer challenges the transaction, the cardholder is required to complete an authentication step, such as entering a static or a dynamic (often one time) password provided by the issuer at the time of the transaction; and

   v) upon the cardholder entering the correct password, the issuer approves the transaction,

   together **3D Secure**.

The CNPF Working Group considered these options and consulted on them with relevant stakeholders across the Australian payments industry, including card issuers and acquirers, card schemes, payment gateways, online merchants, online fraud prevention providers and regulators.

Through this consultation, the CNPF Working Group determined that the industry should progress the implementation of 3D Secure in conjunction with fraud risk thresholds and dynamic cardholder authentication measures (**3D Secure security measures**). This decision was based on the fact that the 3D Secure security measures had the ability to provide for significant improvements in online transaction fraud mitigation. In particular:

a) 3D Secure involves the exchange of authentication information between all relevant parties to a transaction;

b) the use of dynamic authentication measures (such as a one time password) makes it practically difficult to replicate to complete a fraudulent transaction;

c) 3D Secure is an internationally recognised protocol and would keep the authentication of Australian online payment card transactions aligned with global standards; and

d) 3D Secure provides an incentive for merchants to adopt effective fraud mitigation by transferring the liability for financial losses resulting from any fraud on these transactions from the merchant, as is currently the case under the card scheme rules, to the card issuer (usually a financial institution).

It is for these reasons that 3D Secure has emerged as a widely available process for CNPF mitigation and the major global card schemes have each developed 3D Secure processes under scheme specific brands, Verified by Visa, MasterCard SecureCode and American Express Safekey.

3D Secure has been implemented broadly, and sometimes on a mandatory basis, in a number of overseas jurisdictions including the UK and European Union (with the support and encouragement of the European Central Bank) and Singapore (with the mandate of the Monetary Authority of Singapore). However, in most 'voluntary' jurisdictions (e.g. Australia and the USA), the implementation of these processes has been limited.

2.4 3D Secure in Australia

In Australia, 3D Secure was launched to online merchants on a voluntary basis about 10 years ago, with no consistent approach. This caused high variation in the process that the cardholder experienced across different payment schemes, different merchants, different acquirers and different issuers. Although available from the three major global card schemes, all major issuers, payment gateways and acquirers of online transactions, as of today, 3D Secure has not been widely adopted by merchants and the vast majority of online transactions in Australia are not protected by 3D Secure.

It is estimated that only about 3,000 online merchants out of an estimated total of 100,000 online merchants operating in Australia are currently using 3D Secure. Many of the merchants currently using 3D Secure have had to adopt this form of online security, as they have exceeded the fraud thresholds permitted in the rules of the global payment schemes.

A key issue that has limited the introduction of 3D Secure is the extent to which it created confusion for cardholders by imposing an inconsistent and unexpected (due to low adoption) additional step in the transaction process. Inconsistent consumer experience with 3D Secure arose from:

a) a mix of different challenge windows (including pop-up browser windows or redirecting cardholders to the issuer's webpage);

b) the use of static passwords and cardholders having difficulty remembering passwords that they may use infrequently; and

c) a lack of understanding of the need for the 3D Secure process and the steps required to be performed by the cardholder.

In this context, the implementation of 3D Secure in Australia has coincided with a higher level of transaction abandonment by consumers than for transactions where 3D Secure is not applied.

Given the loss in sales associated with transaction abandonment, online merchants have been reticent to adopt 3D Secure. In particular, merchants have expressed concern that the adoption of 3D Secure in circumstances where their rival merchants do not require cardholders to do so may provide a competitive disadvantage. This is despite the fact that there are significant advantages for merchants in using 3D secure, as the liability for financial losses caused by fraud is shifted from merchants to issuers in 3D secure transactions.

In addition, it is understood that some merchants, predominantly smaller merchants, do not appreciate the risks, cost or extent of online payment transaction fraud, and hence perceive that there are greater net benefits to them from increased sales arising from as streamlined a cardholder transaction process as possible. In addition, online retailer groups provided feedback that some merchants were prepared to run the risk of increased fraud and simply build the cost of fraud into their pricing models.

This concern regarding an 'uneven playing field' for merchants has impacted the extent to which financial institutions have been prepared to promote or mandate the use of 3D Secure for online transactions. Acquirers have not wanted to force their merchant customers to apply 3D Secure in circumstances where this could result in a loss of market share to acquirers that are not applying 3D Secure. This dynamic also applies at a Scheme level, with none of the card schemes being prepared to enforce a mandate for 3D Secure on a widespread basis.

2.5 The need for a coordinated approach

After considering the factors that have limited adoption to date, the CNPF Working Group concluded that 3D Secure was still the most effective way to combat CNPF and that an industry-wide initiative would be needed to effectively implement 3D Secure across the Australian market.

It was considered that a coordinated or industry-wide adoption of 3D Secure was necessary in order to:

a) provide for a consistent cardholder experience. It is understood that cardholder acceptance of 3D Secure has been limited by different approaches to its implementation, creating and exacerbating merchant concerns regarding its impact on transaction completion;

b) provide for an effective consumer education campaign. Without a consistent and coordinated implementation, it is difficult to effectively communicate with cardholders as to their role in the process. The potential for cardholder confusion significantly undermines the ability of the industry to demonstrate the benefits of the process to consumers;

c) address merchant concerns regarding the impact of 3D Secure on their competitive position relative to other merchants. It is understood that by ensuring that all merchants are involved and providing a consistent user experience and by using current technology, the key concerns of merchants will be addressed and resistance to the introduction of 3D Secure will be addressed;

d) enabling 3D Secure to operate most effectively. As the fraud risk analytics that are used to identify high risk transactions at the issuer are able to become more precise over time, they will be most effective (and accurate in identifying high risk transactions) where they have the largest sample pool of transactions to analyse. This benefit has flow on effects to the minimisation of the number of transactions that are required to be challenged through the 3D Secure protocol, hence the extent to which cardholders are required to complete an additional step in the transaction process;

e) provide for the most effective approach to online fraud mitigation by enabling the industry to apply fraud risk thresholds on a consistent basis. To the extent that this is not coordinated, varied responses to changes in the level of online fraud would undermine the effectiveness of online fraud mitigation, provide for varied cardholder experiences and confidence in the process and create and revive merchant concerns regarding the impact of the process on competition; and

f) ensure that consumer confidence in the payment system is not undermined by rapidly increasing rates of online fraud.

On this basis, on 16 December 2015, the IAF accepted the CNPF Working Group recommendations to progress the CNPF project to provide for the industry-wide implementation of 3D Secure, subject to regulatory approvals.

The implementation of 3D Secure has achieved broad industry support from financial institutions, card schemes, ACS service providers, payment gateways and the RBA on the basis that it will:

a) overtly demonstrate to Australian cardholders that steps are actively being taken to improve the security of online payment card transactions;

b) be effective in addressing the rapid growth of CNPF;

c) be inclusive in that the APCA structure will enable IAC Framework Participants (**IAC members**) that are involved in the vast majority of CNP transactions in Australia be covered; and

d) reflect a minimum standard for CNPF mitigation without hindering existing or new CNPF initiatives.

3. CONDUCT FOR WHICH AUTHORISATION IS SOUGHT

The conduct for which authorisation is sought involves APCA and those card schemes, issuers and acquirers that form the current and prospective IAC members agreeing to:

a) make changes to the IAC Regulations and Code Set and/or the credit, debit and charge card scheme rules for the sole purpose of implementing 3D Secure security measures to provide for:

   i) the mandatory enrolment in the 3D Secure security measures of both all relevant payment cards issued in Australia and all online merchants in Australia;

   ii) the determination of fraud risk thresholds that are focused on targeting high risk online transactions to determine when 3D Secure should be applied to an online transaction and when such an online transaction should be challenged by the use of dynamic authentication measures; and

   iii) the application of 3D Secure security measures based on fraud risk thresholds to particular online transactions involving particular Australian based merchants in which credit, debit or charge card numbers are entered on the merchant's website;

b) implement the measures in (a) in a common timeframe; and

c) jointly fund and implement a public communications strategy in relation to the proposed arrangements in (a) and (b),

together, the **3D Secure arrangements**.

A list of parties to the proposed arrangement is set out in Attachment A.

The application for authorisation has been structured in this way to address five practical issues.

Firstly, APCA is the natural applicant for authorisation on an industry-wide basis as the structure and membership of the IAC involve the financial institutions and payment card schemes which are involved in almost all CNPF transactions in Australia. Without this structure, it would be more difficult to implement 3D Secure as applications for authorisation by at least APCA and each of the schemes would be required, leaving the potential for complexity and a lack of uniformity. IAC membership is also highly accessible such that any new entrants to online card payments in Australia would, by joining the IAC,

be covered by the authorisation and should they choose to do so, implement 3D Secure in accordance with the industry standard developed in accordance with the authorisation.

Secondly, the scope of the application is targeted in that it is confined to the transactions that make the greatest contribution to CNPF, namely, where cardholders are required to enter their card number into a merchant's website in order to complete the transaction. Other online transaction types, such as those involving digital wallets or those involving card numbers held 'on file' by a merchant for use at their website, have not been included in the scope of the application because CNPF rates on these transactions are significantly lower and at this stage, their inclusion is not considered necessary to deliver the public benefit of reduced CNPF.

Thirdly, the successful implementation of 3D Secure is not possible without comprehensive cardholder and merchant participation. To the extent that significant exceptions are made, or cardholder or merchant participation is optional, it could be expected that the take-up by other merchants would be greatly reduced and CNPF would remain and expand in those areas as a result of fraudsters targeting 'unprotected' transactions.

Fourthly, the greatest benefits of 3D Secure will be realised when sufficient transaction data is available to better identify (and challenge) the highest risk transactions, thereby minimising the extent to which the process involves any additional action by cardholders. As a result, the proposed conduct will involve the development of fraud risk thresholds to identify those online transactions that should result in a challenge to the cardholder, which after full implementation is intended to involve approximately 5 per cent of total online transactions.

Finally, the benefits of implementing 3D Secure are most likely to be realised where the proposed conduct is coordinated with a common timeframe and through a broad communications strategy. This will ensure cardholder confusion and the impact on merchants is minimised.

4. RELEVANT MARKETS

The markets relevant to assessing the application are the payments system markets in Australia in which credit, debit and charge card services are provided by:

a) financial institutions to cardholders and merchants; and

b) card scheme operators to financial institutions.

5. PUBLIC BENEFITS

There are likely to be significant public benefits arising from the proposed conduct. In order to assess these public benefits it is necessary to consider the future with and without the proposed conduct so as to identify the extent to which any benefit to the public is attributable to the proposed conduct.

The future without the proposed conduct is likely to involve:

a) the limited, or at least delayed, implementation and acceptance of 3D Secure as CNPF mitigation measure. The level of adoption of 3D Secure to date both in Australia and overseas demonstrates that:

   i) there are practical constraints that limit the extent to which 3D Secure will be adopted. In particular, cardholder confusion and a reluctance on behalf of merchants to adopt 3D Secure are likely to continue in the absence of the proposed conduct, restricting the effective implementation of 3D Secure; and

   ii) without mandatory implementation of 3D Secure, it is unlikely that these practical constraints can be overcome;

b) as a consequence of limited or delayed implementation, ongoing cardholder confusion and costs to merchants arising from the introduction of multiple approaches to implementing 3D Secure. In particular, cardholder confusion in relation to the ad hoc application of 3D Secure would impact cardholder acceptance of the process and additional resources are likely to be required in order for merchants to overcome this;

c) the continued growth of CNPF and consequent costs, including:

   i) costs to consumers, such as increases in the price of goods purchased online and the cost of payments services, inconvenience in dealing responding to instances of fraud, undermined confidence in the payment system and risks associated with the disclosure of personal information; and

   ii) costs to merchants, in the form of direct costs of financial losses caused by fraud. These costs can be substantial and can jeopardise the business of the merchant. Without the adoption of the 3D Secure arrangements these costs will continue to predominantly be borne by merchants; and

d) undermined consumer confidence in the payment system arising from the increased rate of growth of CNPF. Although payments fraud in Australia is relatively low, it is critical that the integrity of the payments system is maintained and protected by ensuring that payment processes are not easily compromised. To the extent that key areas of fraud are not addressed or are perceived as being incapable of being addressed, this would be likely to have a detrimental impact on consumer confidence in the payment system and through a consequent reduction in transactions, negatively impacting the economy more broadly.

As the proposed 3D Secure arrangements have been developed with reference to these considerations, it is intuitive that the public benefits arising from the proposed conduct are the corollary of the 'future without' scenario. In particular, the public benefits arising from the proposed conduct include:

a) the widespread, or at least faster, adoption of an effective approach to address CNPF in the form of the 3D Secure arrangements. This includes the ability to coordinate the implementation of the 3D Secure arrangements so as to overcome or minimise any negative impact on cardholders and merchants;

b) a reduction in cardholder confusion and costs to merchants arising from an industry-wide consistent approach to addressing CNPF and communicating the 3D Secure process to cardholders;

c) a reduction in CNPF and consequent costs imposed on consumers and merchants. This is because the rates in jurisdictions in which 3D Secure has been introduced on a mandatory basis indicate that it is highly effective in reducing CNPF and the 3D Secure arrangements will be implemented in a manner so as to focus on transactions that are the highest risk of fraud at first instance; and

d) increasing consumer confidence in the payments system and in particular the integrity of online payment card transactions in Australia. Consumer confidence in the payments system is significantly undermined from becoming involved in, or otherwise aware of, payments fraud and the consequent loss of personal information. This is exacerbated in circumstances where the industry and/or regulators are perceived to be incapable of taking steps to address increased payments fraud. The proposed conduct will provide a significant benefit to the public by both reducing CNPF and demonstrating to consumers that the industry is capable of adapting to address emerging fraud risks.

6. PUBLIC DETRIMENTS

The proposed conduct is unlikely to give rise to significant public detriments in terms of an adverse impact on competition, an impact on merchants or an impact on consumers.

In terms of the impact of the proposed conduct on competition, the 3D Secure arrangements are confined in that they apply to a minor dimension of competition in the form of security for online payment card transactions, and only to a limited extent.

The scope of the 3D Secure arrangements only relates to aspects of online fraud mitigation that have not and cannot be effectively addressed through competition and innovation. Importantly, the 3D Secure arrangements provide for a protocol only and do not mandate the use of particular providers of payments service. For instance:

a) issuers and acquirers will continue to have the freedom to use any payment card scheme that they choose, including any new entrants in Australia, whether or not they choose to become IAC members and implement the 3D Secure arrangements;

b) merchants will continue to have the freedom to use any acquirer or payment gateway that they choose, as well as the freedom to implement additional fraud prevention measures;

c) financial institutions will have the freedom to use any ACS service provider that they choose; and

d) online payments providers will continue to innovate and compete for transactions without being hindered or disadvantaged.

Most importantly, IAC members would continue to compete with respect to other more significant dimensions of competition such as fees, terms and conditions for payments services and products. As a result it is highly likely that the impact on competition arising from the proposed conduct would be imperceptible.

In terms of the impact on merchants, it is notable that the 3D Secure arrangements may involve some merchants being required to participate in a process that they do not perceive to be necessary, namely, the mitigation of CNPF. However, any resistance on behalf of merchants is intended to be addressed by the coordinated industry-wide basis upon which the 3D Secure arrangements have been structured. For instance, it is proposed that:

a) as is the case today for those merchants that have implemented 3D Secure, the 3D Secure arrangements will provide for liability for CNPF to be transferred from the online merchant to the issuer;

b) the implementation of the 3D Secure arrangements will be focused on the highest risk categories of Australian merchants in the first instance, and thereafter a staged rollout to all other merchants over a period of at least three years. These high risk categories of merchants correspond with goods or services that may be easily traded for value by fraudsters and include online office school supply and stationery stores (especially where laptop computers can be purchased online and collected almost immediately in store), travel agencies, department stores, clothing stores and household appliances;

c) the 3D Secure arrangements will not be applied to small Australian merchants with a turnover of less than $1 million online until at least 2018 unless they are the subject of exceptionally high fraud rates. It is estimated that merchants with turnover of less than $1 million online form approximately 90 per cent of Australian online merchants;

d) there will be no fees imposed by acquirers on merchants under the 3D Secure arrangements, including fees for the use of 3D Secure related logos. It is possible that the additional activities of payment gateway service providers in relation to 3D Secure transactions may result in an additional fee, but this is likely to be:

    i) offset by the lower interchange fees that are applied by the card schemes for 3D Secure transactions and the lower fraud losses incurred by the merchant; and

    ii) the subject of competition between payment gateway service providers, which, in the context of lower overall costs to the gateway operator, could be expected to result in no fees being applied;

e) the 3D Secure arrangements will be implemented on a consistent basis to categories of online merchants so that particular merchants do not find themselves at a disadvantage by implementing 3D Secure security measures in circumstances where their competitors do not;

f) the 3D secure arrangements will be implemented in a way that will address the inconsistent cardholder experience that has characterised the implementation of 3D Secure in Australia to date and minimise cardholder abandonment of online transactions; and

g) the 3D Secure arrangements will be supported by a consumer education campaign which will drive cardholder understanding of the process.

The proposed conduct will not give rise to any detriments to consumers. In fact, the conduct is significantly beneficial to consumers in providing for increased payment system confidence and security, as well as the protection of personal information. In terms of the ability of consumers to participate in the online payment card transactions process under the 3D Secure arrangements, consumers are likely to require similar capability to complete an online transaction with or without the implementation of the 3D Secure arrangements.

7. CONCLUSION ON PUBLIC BENEFIT

In the context of the significant public benefits directly arising from the 3D Secure arrangements, and the limited public detriments, there are clear net public benefits arising from the proposed conduct.

8. INTERIM AUTHORISATION

8.1 Preparatory steps for which interim authorisation is required

In order to ensure the implementation of the 3D Secure arrangements can be achieved as soon as possible in 2017, APCA requests an interim authorisation for the period from the date of an ACCC draft determination until the final authorisation is granted or refused.

Interim authorisation is required in order for preparatory steps to be undertaken by IAC members, including:

a) make changes to the IAC Regulations and Code Set and/or the credit, debit and charge card scheme rules for the purpose of implementing 3D Secure security measures to provide for the mandatory enrolment in 3D Secure security measures of both all relevant payment cards issued in Australia and all online merchants in Australia. Some of these rule changes are expected to be completed in June 2016;

b) issuers acting in accordance with the changes referred to in a) to enrol all relevant payment cards issued in Australia for the purpose of the 3D Secure arrangements. This process involves the collection of cardholder information (e.g. mobile telephone numbers) and providing this to their ACS service provider. It is estimated that issuers would currently hold accurate full contact details for over 50 per cent of their cardholder customers and that obtaining details from the remaining cardholders will take approximately eight months to complete; and

c) acquirers acting in accordance with the changes referred to in a) to identify the first tranche of Australian online merchants and ensure they are prepared for the

implementation of the 3D Secure arrangements. This process would apply to between 1,000 and 1,500 Australian online merchants that are expected to form the first tranche and will take approximately eight months to complete. The process steps involved are that online merchants would:

i) prepare to make arrangements, or instruct their payment gateway to prepare to make arrangements, for the routing of transactions to an issuer's ACS provider; and

ii) prepare to make changes to their website page design to accommodate the 3D Secure challenge. This is expected to include introducing a new 'iFrame' (box) within the merchants website through which a cardholder could be challenged;

d) commence the development and deployment of a broad communications strategy to prepare for and support the implementation of the 3D Secure arrangements. The proposed steps involved in this are that:

i) the formation of a working group to guide the centralised development of graphic devices and key messages to be used in communications with their cardholders and merchants;

ii) establishing a portal from which a 'communications toolkit' of these graphic devices and key messages may be accessed by stakeholders;

iii) activating the portal to make the toolkit available for the use by stakeholders on a voluntary basis to communicate with cardholders and merchant customers, without charge and with or without modification by stakeholders; and

iv) developing a centralised public relations and advertising campaign to support the use of the communications toolkit by stakeholders.

For clarity, the preparatory steps for which interim authorisation is required would not involve any issuer, acquirer, cardholder or merchant being required to complete an online transaction in accordance with the 3D Secure arrangements.

8.2 Criteria for interim authorisation

Given the extensive timeframes, in particular those referred to in sections 8.1 b) and c), for these preparatory steps to be completed, it is highly preferable that APCA commences the preparatory steps as soon as possible to enable the implementation of the 3D secure arrangements in 2017. In this regard, there is a direct link between the granting of interim authorisation and the earlier implementation of the 3D secure arrangements.

To the extent that interim authorisation could not be obtained to provide for the preparatory steps set out above, then the implementation of the 3D Secure arrangements would need to be deferred, noting that for every month of delay, about $10 million of fraud losses are suffered by Australian online merchants.

The application for interim authorisation is necessary as the proposed conduct is long overdue and necessary in the context of the increasing rates of payment card transaction fraud and particularly CNPF. The industry has allowed a period of 10 years for effective online fraud mitigation technologies to emerge, including the significant implementation of 3D Secure. Prior to the formation of the IAC, APCA and the industry did not have a framework that could effectively facilitate an industry-wide response to CNPF.

The APCA and IAC have wasted no time in progressing the CNPF project and lodging the application for authorisation. In this context, APCA requests the ACCC grant interim authorisation to enable the implementation of the 3D Secure arrangements as a matter of urgency.

In terms of the relevant factors for the ACCC to take into account in considering the request for interim authorisation, it is important that:

a) the proposed conduct would not be anti-competitive. In particular, in the period for which interim authorisation is sought there will be no application of the 3D Secure arrangements to any transaction, other than on an existing or voluntary basis. The steps for which interim authorisation is required are entirely preparatory and would only involve obligations being imposed on issuers, acquirers, payment gateways, relevant online merchants in first tranche and cardholders that are preparatory and/or administrative in nature. There would be no impact on other parties;

b) the cost of the preparatory steps would be limited and there would be very limited cost foregone in the period of two to three months between a draft and final determination in the event that final authorisation was not granted:

    i) in terms of costs to issuers, the preparatory steps required are not substantial and correspond with their independent business need to maintain accurate contact details of cardholders;

    ii) in terms of costs to acquirers, the preparatory steps required are not substantial and require only communications with payment gateways and the first tranche of Australian online merchants; and

    iii) in terms of the costs to first tranche of Australian online merchants, the preparatory steps required are not substantial and involve communications with a payment gateway and minor website changes. As the first tranche of merchants are likely to be larger merchants that update their websites regularly, the costs of making website changes is unlikely to be significant. In the event that any online merchants are included in the first tranche that do not have this capability internally, it is estimated that the cost of making the change required could be between $3,000 and $10,000. However, there is nothing in the preparatory steps that are the subject of an interim authorisation which would require a merchant to make website changes at any particular time. Where a merchant was very concerned as to the cost of making changes to their website then they could elect to defer this step until after a final decision has been made by the ACCC, assuming authorisation is granted;

c) there will be no substantive change to the relevant markets as a result of the preparatory steps for which interim authorisation is required. To the extent that the markets changed at all through the rule changes and enrolment of issued cards and merchants, this would not impact the ability or incentive of IAC members to implement alternative online fraud mitigation arrangements. To the extent that final authorisation is not granted, it could be expected that the same impediments to the effective implementation of 3D Secure in Australia would apply and the likelihood that it would be adopted by a substantial proportion of merchants would remain unlikely;

d) the application for authorisation and interim authorisation has been lodged without delay. Relative to the importance of the CNPF proposal and the number of interested stakeholders, the application for authorisation has been lodged very quickly, reflecting the need for the industry to move quickly to address the growing losses and problems associated with CNPF;

e) significant harm would arise from further delays in effectively addressing CNPF. As a result of the timeframes set out above, a delay of approximately two to three months would arise from the request for interim authorisation being refused. Given the current rates of CNPF and the expected growth in CNPF, the fraud related losses in this period and through the consequent delay in the achievement of the CNPF reduction target would be substantial;

f) the harm arising from the request for interim authorisation being refused would ultimately be met by consumers through as increases in the price of goods purchased online and the cost of payments services, inconvenience in dealing responding to instances of fraud, undermined confidence in the payment system and risks associated with the disclosure of personal information; and

g) the significant net public benefits arising from the 3D Secure arrangements would be facilitated and realised sooner through the request for interim authorisation being granted.

9. TERM OF THE AUTHORISATION

The term of the authorisation sought is 5 years. This term is required in order to provide for the preparatory steps for the implementation of the 3D Secure arrangements as soon as possible in 2017 and the application of subsequent tranches of online merchants over three years until around March 2020. An additional period of 12 months has been incorporated into the term of the authorisation sought in order to avoid the need for reauthorisation in the event that there are practical difficulties in meeting the proposed implementation timeframe.

ATTACHMENT A - PARTIES TO PROPOSED ARRANGEMENT

Current and prospective Framework Participants of the APCA Issuers and Acquirers Community (IAC members) as set out in the table below.

Organisation	**Address**
American Express Australia Limited	12 Shelley Street, Sydney, NSW 2000
Australia and New Zealand Banking Group Limited	ANZ Centre, Level 9, 833 Collins Street Docklands, VIC 3008
Australian Settlements Limited	ASL House, 6 Geils Court, Deakin ACT 2607
Bank of Queensland Limited	Level 17,BOQ Centre, 259 Queen Street, Brisbane QLD 4000
Bendigo and Adelaide Bank Limited	The Bendigo Centre, Bendigo VIC 3550
Cashcard Australia Limited	Level 11, 168 Walker Street , North Sydney NSW 2060
Citigroup Pty Limited	GPO Box 40, Sydney NSW 2001
Coles Group Limited	Level 5, Module 1, 800 Toorak Rd, Tooronga VIC 3146
Commonwealth Bank of Australia	Level 6, 201 Sussex Street, Sydney NSW 2000
Cuscal Limited	Level 1, Margaret Street, Sydney NSW 2000
eftpos Payments Australia Limited	Level 9, 60 Carrington Street, Sydney, NSW 2000
Indue Limited	Level 3, 601 Coronation Drive, Toowong QLD 4066
MasterCard Worldwide (Australia) Pty Ltd	Level 8, 100 Arthur Street, North Sydney, NSW 2060
National Australia Bank Limited	Level 3 (UB 3350), 800 Bourke Street, Docklands VIC 3008
Suncorp-Metway Limited	Level 18, Suncorp Centre, 36 Wickham Terrace, Brisbane QLD 4000
Tyro Payments Limited	1, 155 Clarence Street, Sydney NSW 2000

Westpac Banking Corporation	Level 20, 275 Kent Street, Sydney NSW 2000
Woolworths Limited	1 Woolworths Way, Bella Vista NSW 2153
Visa AP (Australia) Pty Ltd	Level 42, AMP Centre, 50 Bridge Street, Sydney, NSW 2000
Any other organisation which becomes an IAC member	