Our Ref: 59196
Contact Officer: Michael Drake
Contact Phone: (03) 9658 6517

24 March 2016

Australian Competition & Consumer Commission

GPO Box 3131
Canberra ACT 2601

23 Marcus Clarke Street
Canberra ACT 2601

tel: (02) 6243 1111
fax: (02) 6243 1199

www.accc.gov.au

Rowan McMonnies
Partner
Baker & McKenzie

***By email**:* Rowan.McMonnies@bakermckenzie.com

Dear Mr McMonnies

Australian Payments Clearing Association applications for authorisation (A91525 & A91526) – further information request

Thank you for the Australian Payments Clearing Association's (APCA) supplementary submission of 11 March 2016 in response to submissions received from interested parties on the applications.

The ACCC has identified a number of areas in which we consider more information is required. We consider that the additional information is necessary in order to understand the arrangements for implementation of the proposed conduct and the context in which it will take place and, ultimately, to enable us to assess the extent to which the proposed conduct is likely to result in public benefits and/or public detriments.

Given the nature of the information requested we ask that you provide a written response. The written response, along with any documents provided in response to the information request, will be placed on the ACCC's public register, subject to any request for exclusion.

For clarity, any reference to '3D Secure' in this request refers to current and future versions of 3D Secure, including the '3D Secure 2' product foreshadowed in APCA's 11 March 2016 submission.

Request for further information

1. Access to 3D Secure and financial arrangements for 3D Secure

   i. Please provide a detailed explanation of the current access arrangements for 3D Secure. Please include a description of the process for seeking access and the cost of access.
      (a) Does anything in the terms of access dictate through which payment channel a transaction using a multi-network card is routed?

   ii. Please set out any anticipated future changes to the access arrangements for 3D Secure. Please include a description of changes that may occur if the proposed conduct is authorised and if EMV Co becomes the rights holder to 3D Secure.

   iii. Please set out the existing and proposed revenue sources for the owner of 3D Secure – including which parties it would recover revenues from; and the structure (i.e. one-off fixed charge, annual fee, ongoing per transaction fee, etc.) and level of

all existing and proposed charges. Please describe how the proposed conduct (if authorised) will affect the revenue earned by the owner of 3D Secure.

iv. APCA states in its March 2016 submission (p.9) that the 3D Secure arrangements are 'readily available and accessible to market participants'.
   (a) Does APCA have any control—direct or indirect—over access to 3D Secure?
   (b) Are there any restrictions on what the owner of 3D Secure is able to charge for access to the product?
   (c) Are there any restrictions on how the owner of 3D Secure can alter the structure of charges for access to the product in the future, including which parties it would recover its costs from?

v. APCA also states in its March 2016 submission (p.9) that 'it would not be possible for APCA to achieve its objectives of addressing online transaction fraud if market participants are unable to obtain access to 3D Secure'.
   (a) If, in the future, a new market participant (e.g. a new payment scheme or new issuer/acquirer) was unable to access 3D Secure, or expressed concerns over the terms on which they were being offered access, how would APCA address that issue, and how would it affect APCA's approach to the proposed conduct?

2. Costs for merchants

i. Please set out how APCA intends to define and identify 'online merchants in Australia'.

ii. APCA states in its January 2016 submission (p.19) that the estimated costs to the first tranche of merchants to update their websites would be between $3000 and $10,000, for merchants which lack internal capability to effect the change.
   (a) How has APCA estimated these figures?
   (b) What are the cost components that make up the $3000-$10,000?

iii. Where costs may differ between different types or sizes of online stores, or based on the gateway provider selected by each merchant, please explain and estimate cost differences.

iv. APCA states in its March 2016 submission that merchants are not required to obtain the 3D Secure product or licence (p.7). Is the intellectual property that allows for 3D Secure to be integrated into online stores monetised? If so, who pays for access to that IP?

v. Under the proposed conduct, each Australian online merchant, of which APCA submits there are approximately 100,000, will be required to incur costs of implementing 3D Secure. As noted above, APCA estimates these costs are between $3000 and $10,000, but may differ depending on the particular merchant. This suggests an overall cost to online merchants of between $300 million and $1 billion.
   (a) How has APCA calculated that the proposed conduct would result in benefits that outweigh such a cost to online merchants? Please provide any relevant documents to support these calculations.

vi. We understand that the proposed 3D Secure arrangements would not be applied to merchants with a turnover of less than $1 million online until at least 2018 unless they are the subject of 'exceptionally high fraud rates'.
   (a) Is it the intention that the proposed conduct would apply to very small 'online stores' (e.g. stores that generate less than $10,000 per year such as, for example, the neighbourhood tennis courts that can be booked online)?

3. The 3D Secure product

   i. Please provide any reports available to APCA, including reports that focus on contexts outside Australia, that:
      (a) assess the efficacy of 3D Secure in reducing fraud (including the extent to which its implementation led to a reduction in online CNPF); and/or
      (b) assess the costs or experience of using 3D Secure for merchants or consumers.
   ii. Please provide details of any hacks or incidents where 3D Secure has been compromised.

4. Other options considered by APCA to address CNP fraud

   i. Please provide the consultant report that informed APCA's choice of 3D Secure as the appropriate fraud mitigation technology to implement.
   ii. Please provide any other internal APCA documents that assess the different options APCA considered to address CNPF.
   iii. If the proposed conduct were not authorised, what other options would APCA be likely to consider to address CNPF? For example, would APCA further consider the options listed in its January 2016 submission (p.8)?
   iv. APCA's March 2016 submission (p. 5) notes that '3D Secure represents the only fraud security measure that the industry can effectively implement in a short time frame'. Please provide further explanation and information regarding this statement. For example, what were the estimated time frames for implementation of the other options considered by APCA such as data analytics and tokenisation?
   v. APCA's March 2016 submission (p. 4) notes that 'it would be prohibitively expensive for the vast majority of merchants to implement alternative security measures to meet a security standard at a comparable level to that of 3D Secure'. Please provide further information to support this statement. For example, what are the costs for merchants to implement the alternative security measures, and how do they compare to 3D secure?

5. Fraud risk thresholds

APCA's March 2016 submission notes that 'the fraud risk thresholds that would apply in the context of the 3D Secure arrangements will not be formally considered and adopted by the IAC until after interim authorisation and/or authorisation has been granted by the ACCC. However, a proposed structure has been developed as part of the proposal to implement the 3D Secure arrangements subject to the authorisation being obtained.'

   i. Please provide a copy of the proposed structure.
   ii. Please set out the process for amending the fraud risk thresholds during the authorisation.

6. International experience

   i. APCA states in its January 2016 submission that '3D Secure is an internationally recognised protocol and would keep the authentication of Australian online payment card transactions aligned with global standards'. (p.9) What are the global standards referred to here?

ii. Page 9 of the January 2016 submission notes that 'many 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.' What are these rules/who sets them/and what are the fraud thresholds?

iii. Page 9 of the January 2016 submission also notes that '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).

(a) In those jurisdictions in which 3D Secure is mandatory for online merchants, what is the scope of the mandate (i.e. are there exceptions for particular categories of online merchants)?

Next steps

We would appreciate it if you could provide this information by Friday, 8 April 2016.

In providing a response, please clearly identify any information that APCA wishes to have excluded from the public register and provide brief reasons for any exclusion sought.

This letter will be placed on the ACCC's public register.

If you wish to discuss any aspect of this matter, please contact Michael Drake on (03) 9658 6517 (michael.drake@accc.gov.au) or me on (03) 9290 1973 (lyn.camilleri@accc.gov.au).

Yours sincerely

Lyn Camilleri
Director
Adjudication