:86 400

Australian Securities & Investments Commission

By email : ePaymentscode@asic.gov.au

3 April 2019

Submission by 86 400 Ltd in response to Consultation Paper 310 Review of the ePayments Code: Scope of Review

86 400 Ltd (**86 400**) welcomes the opportunity to provide feedback on ASIC's consultation paper 310 (**CP 310**).

86 400 was founded in 2017 by Cuscal Limited (**Cuscal**) and is currently 100% owned by Cuscal. Cuscal in turn is largely owned by Australian challenger banks and customer-owned banks.

After conferment of a licence to operate as an authorised deposit-taking institution, 86 400 intends to offer a range of deposit and credit products. 86 400 will be a digital bank which intends to stay at the forefront of technology enabled banking services and from launch will be deploying advanced payment methods including NPP, Apple Pay, Google and Samsung Pay as well as traditional direct entry transfers.

86 400 has not subscribed to the ePayments Code (**the Code**) but has developed its processes to be generally consistent with the current Code. We expect to be subject to an updated version of the Code, whether through subscription or the mandatory application of that Code.

In this submission we have limited our comments to those aspects of CP 310 where we have a strong view as an intended future Code participant. Those aspects are related to account aggregation.

Account Aggregation and Customer Liability

We are pleased to see ASIC's recognition of the consumer benefit in the use of aggregation services. We see these services currently as being entirely consistent with the Customer Data Right (**CDR**)and a precursor to the Open Banking regime which we agree will ultimately, over time, supersede the need for reliance on "screen-scraping".

We fully support the aims of the Open Banking legislation which are well summarised in the following passage from the Explanatory Memorandum to that legislation:

> *"The primary aim of the CDR is to give consumers the ability to access and use more information about themselves, and about their use of goods and services, in a manner that allows them to make more informed decisions about both themselves and the good and services they use. By doing so, the CDR aims to increase competition, enable consumers to fairly harvest the value of their data, and enhance consumer welfare."*[1]

We believe however, that the current timetable, and practicalities of the full implementation of Open Banking means that it will be some years before screen-scraping can be fully replaced. In the interim the use of properly implemented screen-scraping can achieve much of the aims of the CDR. We do not think that consumers should be discouraged from using a service that benefits them and has the potential to increase competition in the banking industry.

[1] Explanatory Memorandum to the *Treasury Laws Amendment (Consumer Data Right) Bill 2019*

Although a significant number of consumers are already taking advantage of screen-scraping based aggregation services, much of this usage is currently through service providers which are not Code subscribers and which operate outside of financial services regulation. It is our belief that the current uncertainty created by the liability provisions within paragraphs 12 of the Code is discouraging widespread uptake of these services within the regulated sector. We think there is danger in regulation which has the effect of shifting financially related services outside of the consumer protection mechanisms of the regulated sector.

While there are different methods of data transfer and encryption used, all screen scraping technologies require a consumer to input their banking credentials (e.g. password or passcode) at some stage in the aggregation process.

Some uses of aggregated information require that a customer' credentials be stored (in encrypted form) so that they can be used on more than one occasion (e.g. to give a customer a daily view of their balances across multiple financial institutions). Some aggregation solutions hold this data within a centrally held database operated by the aggregator. Other solutions store the information on the consumer's device so that it is never transmitted to the aggregation service provider. Alternative solutions pass through banking credentials with no long term storage.

It is our view that the critical component of all of these solutions is the security of the consumer's data, whether in transit or at rest.

We have had the opportunity to review and analyse a number of offerings from the leading aggregation service providers. Each of these service providers recognises that the protection of customer data is at the core of their business model and have implemented best in class security measures to ensure the protection of customer banking credentials as well as the customer information that is produced during the aggregation process.

We strongly support ASIC's recognition (at paragraph 63 of CP 310) of the need to strike a balance between:

a) providing useful outcomes that take into account customer behaviours; and
b) allowing ADI's to expect reasonable behaviours by their customers to guard against financial losses.

In the context of account aggregation, we believe that the Code could be updated to achieve this by recognising that the input of passcodes in order to use a data aggregation service will not automatically shift liability back to the customer.

We recognise that most aggregation service providers are not subject to any licencing regime in Australia and there is the potential for entrants to offer services without the strong protections which we have observed from the market leaders. For that reason, we believe that a Code amendment of this type must have some limitation to ensure that extremely high quality data security controls have been put in place by the aggregator.

How might the balance be achieved?

We think that it would be appropriate for consumers to be free of liability when using their passcode in connection with an aggregation service where the aggregation solution:

a) does not involve the transfer of pass-code information to any party other than the customer's financial institution;
b) does not provide a means to alter information held at the customer's financial institution;
c) does not provide a means to initiate a financial transaction on the account held at the customers' financial institution;

d) does not provide the means to retrieve the customer's credentials for the use by any other party; and
e) the aggregation provider meets certain security standards (in this respect we suggest the application of SOC 2 type 2 or ISO 27001 standards with attestations specific to the aggregation solution). We would expect that compliance with these standards would be independently certified.

We think that this is a reasonable framework that does not require a large administrative burden, however, the framework could also be extended to require a more holistic accreditation. We think that the proposed accreditation mechanism for Open Banking *(*as set out in the *Consumer Data Right – Rules Outline December 2018)* could be easily adapted to cover entities wishing to rely on screen scraping technology and that the Code could recognise this accreditation.

We offer these alternatives for ASIC's consideration though we expect that there will be other alternatives which would achieve an equivalent balance.

We hope these comments have been useful to ASIC in planning the scope of the review. Please let us know if we can be of further of assistance.

Yours sincerely

Scott Jamieson
Head of Compliance

Brian Parker
Chief Information Officer