AUSTRALIAN
RETAIL
CREDIT
ASSOCIATION

5 April 2019

Australian Securities and Investments Commission
By email

Review of the ePayments Code: Scope of the review

Thank you for the opportunity to provide a submission on Consultation Paper 310: Review of the ePayments Code: Scope of the Review (CP310).

This submission provides commentary and recommendations in relation to the 'account aggregation' issue raised in CP310 – where that service depends on the consumer providing the pass code to their internet banking service (i.e. 'screen scraping').

The improved availability of reliable and meaningful data is good for competition and for consumers. While the Consumer Data Right/Open Banking regime will provide an additional, secure and highly regulated method of data exchange, other forms of data exchange already exist and will continue to co-exist with the CDR regime – such as proprietary API technologies and lower-tech methods like the customer manually sending PDF account statements via email, or even posting paper copies of statements. The Farrell Review into Open Banking in Australia noted in Recommendation 1.1, that allowing competing approaches to the Open Banking regime "…will provide an important test of the design quality of Open Banking and the Consumer Data Right."

As noted in CP310, screen scraping, in conjunction with income and expenses analytics services, are being used as a tool to assist lenders to meet their responsible lending obligations under the NCCP. Should the CDR regime come into place, then the need for such account aggregation services to operate through screen scraping should decrease.

Lack of regulatory framework

Currently, apart from the broad requirements of the Australian Consumer Law and Privacy Act, providers of screen scraping services are currently unregulated. Despite this lack of specific regulation, ARCA is aware of several existing screen scraping services which, based on our dealings with those businesses, appear to be reputable and have appropriate systems and processes in place.

Nevertheless, there is the potential for less reputable and competent providers of screen scraping services to cause real harm to consumers. For example, a provider that did not maintain adequate security controls could be subject to a wide-scale loss of data through hacking.

GPO Box 526, Melbourne, VIC, 3001 | (03) 9863 7859 | info@arca.asn.au | www.arca.asn.au | ABN 47 136 340 791

Similarly, the use of the data obtained by lenders through screen scraping is subject only to the Australian Privacy Principles (in contrast to the strict regulatory restrictions that will be imposed under the CDR regime). While we expect most lenders will use the data appropriately, there is still the potential for consumer's data to be misused.

To date, the risk associated with screen scraping services do not appear to have caused significant harm to consumers. However, should ASIC, through this review or the review of RG209 be seen to accept or endorse practices such as the disclosure of pass codes, there is likely to be a significant uptake in the number of lenders adopting the technology and providers offering the service – some of which are likely to be less reputable or competent. In the absence of specific regulation, the risk of such users or providers causing harm to consumer will increase significantly.

> **Recommendation:** In light of the growing use of screen scraping services, ASIC should, as a starting point, consider establishing best practice principles for the operation of screen scraping services (including competency, security and insurance expectations) and consider ways to promote the adoption of those principles, including working with both the providers of the services and the users of those services (e.g. holders of Australian Credit Licenses). If this approach is not successful, regulatory intervention may be required.
>
> **Recommendation:** Once a regulated approach to data exchange such as the CDR is in operation and adoption widespread, at that time regulation should be reviewed to determine if the benefits of allowing screen scraping outweighed the potential detriments.

Liability implications of account aggregation services

By voluntarily providing their pass code to the screen scraping service, the consumer has arguably breached the pass code security requirements in clause 12 of the Code and the terms and conditions of the internet banking service offered by their bank. As a result, the consumer may be liable for the losses that result from that breach[1].

Accordingly, the consumer may be liable for loss that arises from an unauthorised internet transaction resulting from a breach of security or some other cause at the screen scraping service. This is unlikely to occur at a reputable and competent service which maintains appropriate security controls[2]. As noted above, consideration should be given to developing best practice principles for screen scraping services to mitigate such risks.

While the risk of loss is low, we believe that it would still be appropriate to review the issue of liability under clause 11 given the potential for a number of parties to be responsible or 'at fault' for any loss. The ePayments Code currently determines liability for unauthorised transactions as between the consumer and the subscriber (noting that the actual party

[1] We note that it has sometimes been said that the breach of the security requirements makes the consumer liable for 'any' loss. This is, of course, incorrect as the consumer is only liable for loss that results from their breach.
[2] We note also that, should a bad actor gain access to the consumer's internet banking account as a result of a failing by the screen scraping service, the two-factor authentication utilised by many deposit institutions would protect against loss.

GPO Box 526, Melbourne, VIC, 3001 | (03) 9863 7859 | info@arca.asn.au | www.arca.asn.au | ABN 47 136 340 791

causing the loss, i.e. the fraudster, is unlikely to be identifiable). In respect of losses resulting from a breach of security or some other cause at the screen scraping service, there are an additional two entities that may share some or all responsibility for the loss, i.e. the credit provider to whom the consumer made an application for credit and the provider of the screen scraping service that the credit provider utilised. Depending on the type of credit applied for, the credit provider may hold an Australian Credit Licence and be a member of the Australian Financial Complaints Authority (AFCA). The provider of the screen scraping service is unlikely to be a holder of a licence or be a member of AFCA. Clarification of which parties are liable would be useful.

> **Recommendation:** The issue of liability under clause 11, as it relates to the use of screen scraping services, be reviewed.

Risk of changing consumer behaviour

A further concern regarding security, is that the existence of screen scraping services is undermining a long-held banking industry practice of never asking the consumer to divulge pass code other than in 'secure' situations. The concern is that this, in turn, may result in consumers being less wary when asked to disclose their pass codes in other circumstances – opening the consumer up to greater potential of being defrauded. This becomes a concern of all industry participants as fraud losses may increase.

> **Recommendation:** Consideration be given to providing specific information, that is consistent across subscribers, to consumers regarding screen scraping services with the annual consumer warning required by clause 8 of the ePayments Code. That information could be informed by consumer research undertaken to understand how the use of screen scraping services impacts consumer's susceptibility to potentially fraudulent behaviour.

We would be very happy to provide any further information or clarification that you require.

If you have any questions about our feedback, please feel free to contact me Michael Blyth.

Yours sincerely,

Mike Laing
Chief Executive Officer

GPO Box 526, Melbourne, VIC, 3001 | (03) 9863 7859 | info@arca.asn.au | www.arca.asn.au | ABN 47 136 340 791