AMERICAN EXPRESS

12 April 2019

By Email: ePaymentsCode@asic.gov.au

Dear ASIC,

Review of the ePayments Code

American Express Australia Limited (**American Express**) welcomes the opportunity to comment on the ePayments Code.

American Express

American Express is one of the largest global payment providers and has operated in Australia since 1954. American Express holds an Australian Financial Services Licence and an Australian Credit Licence. American Express is committed to innovation in payments and financial services and is keen to see the ePayments Code evolve to meet the challenges of Australia's Open Banking future.

Account Aggregators

As ASIC has observed, the status of Account Aggregators under the ePayments Code is far from clear. It is arguable that the Code already provides some protection to consumers who use Account Aggregators. Under section 12.9, if a Subscriber were to 'implicitly endorse' an Account Aggregator service, a user would not breach the pass code security requirements under the Code by using that Account Aggregator service. Given that many subscribers currently use Account Aggregators within their own businesses, it could be argued that when they use those Aggregators they are implicitly endorsing them. For example:

> *Bank A uses Aggregator Y for an income/expense verification tool in order to issue that person a credit card. Where a customer then uses a PFM Mobile App powered by Aggregator Y, the customer may well argue that they have not breached pass code security requirements when sharing their credentials with the PFM Mobile App on the basis that Bank A implicitly endorses Aggregator Y.*

It is of course, a bit of a 'grey area'. We consider that an ePayments Code with 'grey areas' does not meet the needs or expectations of the community. Consumers deserve certainty when using and engaging with the increasing range of Account Aggregator services available.

We note that a number of Account Aggregators incorporate strong data security systems, processes and software as core parts of their business.

Despite the imminent roll out of the Consumer Data Right (CDR) in Australia, we agree with ASIC's observation that "…Account Aggregators may remain relevant for some time and coexist with Open Banking". It is therefore important for the Code to address the issue of Account Aggregators at this point in time.

As the Code stands, consumers who use Account Aggregators are in a position where they do not know with certainty whether they will be on the hook or not for unauthorised transactions. The Code imposes a requirement on the consumer, essentially, to do their own data security due diligence on an Account Aggregator. This situation should not persist.

American Express recommends that ASIC give consideration to a de-facto accreditation or recognition framework. This could be achieved simply as follows:

- Include a provision in the Code that acknowledges that where a user shares their pass code with an Aggregator Service (as defined under the Code), the user does not breach the pass code requirements.
- The Code would then include an industry standard definition of Aggregator Service that includes minimum requirements designed to protect consumers and subscribers. For example, the definition of 'Aggregator Service' might:

    - Include 'read access' models
    - Exclude 'write access' models
    - Mandate minimum security requirements (for example, 128 bit encryption)
    - Include any other minimum requirements deemed appropriate in consultation with stakeholders and industry

Consultation on appropriate standards could form part of the next stage of submissions on the Code.

We are not proposing a unilateral endorsement of Aggregator Services in Australia. Nothing in the Code could or should oblige a subscriber to integrate with or make data available to an Aggregator Service. Similarly, nothing could or should prevent a subscriber from blocking access to its sites and services by Aggregators.

Taking this a step further, consideration might also be given to whether the Code could recognise a right on the part of Subscribers to 'black list' specific Aggregator Services and expressly prohibit its customers from sharing pass codes with those Aggregators. Of course, subscribers would need to balance their 'blacklisting' decisions against the increasing need and desire of their customers to use Aggregator Services.

By removing the possibility under the ePayments Code of liability for consumers using Aggregator Services, subscribers will be well motivated to explore safer, more secure and more efficient methods of data exchange with those Aggregator Services. We would expect that this will result in greater collaboration and partnership with Aggregator Services which will have benefits for consumers and businesses alike.

Extension to Small Business

American Express has long been a supporter of small business in Australia with its Shop Small initiative, a national annual movement to encourage more Australians to support small businesses within their local communities.

American Express fully supports the extension of the ePayments Code to small businesses. Small business has the same interest as consumers in avoiding liability for unauthorised transactions.

Shared Devices & Fingerprints

The ability to register multiple individuals to a single mobile device creates challenges given the increasing uptake of mobile wallets. We have always considered that a device owner is best placed to make decisions about device security and access. In circumstances where an individual has permitted another person to use or access their device in such a way that would allow them to make payments, then that transaction should be deemed authorised by that individual. We do not consider it appropriate or desirable for subscribers to police matters around shared devices amongst family and friends.

American Express would be more than happy to discuss any part of this submission in more detail. Please contact Julian Charters or Sarah Wood for further information.