Acorns Grow Australia Limited
Level 11, 2 Bulletin Place
Sydney NSW 2000
T 1300 954 678
www.acorns.com

18 March 2018

To: Open Banking Review Secretariat
The Treasury
Langton Crescent
PARKES, ACT 2600

From: George Lucas
Chief Executive Officer
Acorns Grow Australia Limited
Level 11/2 Bulletin Place
SYDNEY, NSW 2000

Acorns Australia (**Acorns**) welcomes the opportunity to put forward a second submission to the Review into Open Banking in response to the recommendations in its December 2017 Report and also notes its earlier submission to the Review into Open Banking in response to its Issues Paper.

Acorns' responses to the Open Banking's recommendations are set out in more detail in this submission.

Open Banking regulatory framework

Recommendation 2.6 – a Data Standards Body

A Data Standards Body should be established to work with the Open Banking regulators to develop Standards. This body should incorporate expertise in the standards-setting process and data-sharing, as well as participant and customer experience.

Acorns submits that the development of the Standards by a Data Standards Body should involve consultation with both large banks and alternative non-bank providers and agrees that participant and customer experience should be incorporated in the Data Standards Body to avoid, as noted in the Report, conflicts between the commercial considerations of financial institutions and the interests of consumers in Open Banking.

The scope of Open Banking

Recommendation 3.8 – application to ADIs

The obligation to share data at a customer's direction should apply to all Authorised Deposit-taking Institutions (ADIs) other than foreign bank branches. The obligation should be phased in, beginning with the largest ADIs.

Recommendation 3.10 – eligibility to receive data

Authorised Deposit-taking Institutions (ADIs) should be automatically accredited to receive data under Open Banking. A graduated, risk-based accreditation standard should be used for non-ADIs.

Acorns agrees that the obligation to share data at a customer's direction should apply to all ADIs (recommendation 3.8) and that ADIs should be automatically accredited to receive data under Open Banking (recommendation 3.10). However, we submit that the automatic accreditation should also extend to Responsible Entities of registered managed investment schemes, given that both ADIs and Responsible Entities are subject to similar standards and requirements to:

(a) maintain adequate risk management systems under the Corporations Act; and

(b) maintain and adhere to stringent privacy standards under the Privacy Act and the Australian Privacy Principles when collecting and handling personal information.

Responsible Entities follow the cyber security best practices outlined by ASIC, which are on par with cyber security practices at ADIs. At Acorns, we have an external constant evaluating our cyber security, and not only independent penetration testing, but also independent testing our procedures around phishing, USB and other procedural cyber security issues.

The information we collect is stored on secure servers following ISO27001/ISO27018 controls that are protected in controlled facilities. When you log into our websites or apps, 256 bit encrypted data is sent from your computer or phone to our systems. We have VPNs, firewalls, intrusion detection and virus scanning tools to stop viruses and unauthorised people accessing our systems. When we send electronic data to other organisations, we use secure tunnels (VPN and whitelisted IPs) or 256 bit encryption. We also use MFA, VPNs and whitelisted IPs to stop unauthorised people gaining access to the systems.

Extending automatic accreditation to Responsible Entities will not undermine confidence or customers' trust in the security of data sharing in Open Banking – indeed it would be the reverse. If Responsible Entities were required to go through a separate, graduated, risk-based accreditation standard, this will be an impediment to opening up access to customer data to alternative non-bank providers and would be a disappointment to our customers in the short term, given our stringent security and privacy standards that are on par with the large banks.

It would also be an unnecessarily onerous requirement and significantly disadvantage Responsible Entities. Given that Responsible Entities are also subject to regulatory compliance requirements, including those associated with privacy and data maintenance, there should definitely be a level playing field as between ADIs and Responsible Entities in relation to automatic accreditation.

Further, having a separate accreditation for Responsible Entities would imply in the customer's mind that the standards of cyber security, privacy and risk management are different for ADIs and Responsible Entities and that ADIs are held accountable to a higher standard, which is not necessarily the case (as highlighted above). Consumer confidence in the institutions that create the ecosystem of our financial services is of critical importance if Open Banking is to succeed and replace current technologies.

Safeguards to inspire confidence

Recommendation 4.5 – customer control
A customer's consent under Open Banking must be explicit, fully informed and able to be permitted or constrained according to the customer's instructions.

Recommendation 4.6 – single screen notification
A data holder should notify the customer that their direction has been received and that the future use of the data by the data recipient will be at the customer's own risk. The notification should be limited to a single screen or page. Data recipients should similarly provide the customer with a single screen or page summarizing the possible uses to which their data could be put and allow customers to self-select the uses they agree to.

Acorns agrees with recommendation 4.5. However we seek clarification on the form of 'explicit' consent that is required from customers. We submit that explicit consent should permit the bundling of consent for future uses of a customer's data. Customer self-selection as set out in recommendation 4.5 should allow for wide-ranging consent to cover current as well as future permissions. A key feature of the services that Acorns provides to our customers is to offer different financial products as customers' finances and needs change. We continually tailor our products to these changing needs, which cannot be separately listed at the time of obtaining explicit consent, as Acorns will not know what the customer's needs are, or will be, at the time the customer provides explicit consent.

Acorns' proposition is that it 'grows' as the customer 'grows' and as their life changes – therefore, it needs to be able to offer financial products and services that reflect the customer's stage of life – and this is what the customer is, in part, signing up for when they sign up to Acorns. Therefore, the explicit consent should be obtained from the customer at the beginning of the relationship when the customer signs Acorns' Terms & Conditions, and should be for a range of financial products and services that may be offered in the future.

To prohibit the bundling of explicit consent will discourage competition by placing alternative non-bank providers at a disadvantage to large banks, who are not currently required to bundle consents when data is used to cross promote financial products and services. As we will not be able to offer or provide services for customers to make better choices as their needs for these products arise, we will instead be needing to seek consent from customers to inform them of each individual offer or service, which will reduce the impact and practicality of being able to offer competitive products to benefit consumers, and will create additional cost to Acorns – cost which will ultimately be passed onto the customer.

We also note that requiring individual explicit consent for each product or service offered will place the financial services industry at a distinct disadvantage when compared with the big technology players like Google, Facebook and Amazon, who are now collecting payment transaction data through their platforms.

These large tech players offer and cross-promote just as many financial and insurance products as FinTechs in general - but are not subject to a requirement for explicit consent for each individual product / service. Therefore subjecting the financial services industry to such a requirement would create an unlevel playing field and be inequitable to the financial services industry.

Data transfer mechanism

Recommendation 5.1 – application programming interfaces

Data holders should be required to allow customers to share information with eligible parties via a dedicated application programming interface (API).

Acorns understands and endorses the importance of all participants in Open Banking feeling justifiably confident in the system as new technologies and frameworks emerge. However confidence and trust in current technologies is just as important. Acorns submits, and supports the current position adopted by Open Banking, that Open Banking should not expressly prohibit screenscraping, especially during a transition period to the dedicated APIs. Acorns further submits that screenscraping should be used as a benchmark to monitor the performance of Open Banking (in particular, is Open Banking as easy to use as screenscraping; does it provide the same level and quality of information; and are the ADIs liable for the accuracy and timeliness of the information).

As a FinTech, Acorns uses screenscraping, via the aggregator Yodlee, to access our customers' data from their existing banking accounts. The development of screenscraping has arisen because there have not been open APIs to facilitate the transfer of customer data between data holders and data recipients. Moreover, screenscraping uses the information that is available to a customer through their online banking facility. Consequently, this information is up to date and real-time (and banks are liable for the accuracy and timeliness of this information).

While Open Banking does not prohibit or endorse screenscraping, it aims to make this practice redundant by facilitating a more efficient data transfer mechanism. In order for Open Banking to truly empower consumers to use their data to be able to make better financial decisions, it will be fundamental to Open Banking that the dedicated APIs have the simplicity of screenscraping, with real-time and near real-time information. It is also imperative that the data is shared in a format that can be easily used by data recipients to provide benefit to consumers. Lastly, it is also imperative that the provider of the information is liable for the accuracy and timeliness of the information, in the same way as ADIs are currently responsible and liable for the accuracy and timeliness of account information provided to consumers through their online banking facilities (which is what is viewed by 'screenscrapers', and hence provides a high level of certainty that the information is up to date and accurate).

Recommendation 5.5 – no additional barriers to authorisation

Data holders may not add authorisation requirements beyond those included in the Standards. Requiring multifactor authentication is a reasonable additional security

measure, but it must be consistent with the authentication requirements applied in direct interactions between the data holder and its customers.

Acorns submits that requiring multifactor authentication for read transactions is not a reasonable additional security measure in all interactions. Multifactor authentication should only be required during the 'sign up' phase with the customer. At this stage, Acorns agrees that this is a reasonable security measure.

However, requiring multifactor authentication for every read transaction and read interaction past this initial 'sign-up' point is impractical. For example, when Acorns reads our customers' accounts nightly for real-time transactions, to update our roundup service for example, it would be unworkable to require multifactor authentication from our customers in this interaction, and would place us at a competitive disadvantage in the services that we are able to offer. Acorns also submits that it is not necessary to have multifactor authentication each time an individual read transaction occurs to ensure security of the customer's account or information. Multifactor authentication is only necessary for this purpose on the initial sign up phase or write transactions.

We believe this extra layer will add friction online and reduce the adoption rate of Open Banking APIs by consumers.

Recommendation 5.6 – persistent authorisation
Customers should be able to grant persistent authorisation. They should also be able to limit the authorisation period at their discretion, revoke authorisation through the third-party service or via the data holder and be notified periodically they are still sharing their information. All authorisations should expire after a set period.

Acorns agrees with the recommendation 5.6 that customers should be able to grant persistent authorisations for customer convenience. Acorns submits that the set period for authorisations be two years, with an obligation on data holders to notify data recipients of that expiration one month prior to the authorisation expiry date, so that data recipients are able to obtain further ongoing consent from their customers before the scheduled expiry date.

However, we bring to your attention that if the aim of Open Banking is to provide benefits to as many consumers of financial services as possible, then every extra addition of friction of using Open Banking applied to the customer, requiring an input by them, and not the institution, means that the adoption rate of Open Banking and therefore the benefits to the consumer will be reduced significantly.

At Acorns, the rule of thumb that we use is that for every extra piece of information asked for online, we lose 10% to 20% of customers out of the funnel.

<u>Conclsuion</u>

We believe this Review can achieve the required outcome, which will result in a stronger Australian economy delivering better more competitive financial services outcomes for all its citizens – especially young Australians and Australia who have limited acess to competitve financial services.

Yours faithfully,

George Lucas