24 July 2020

Australia Competition and Consumer Commission
GPO Box 3131
Canberra ACT 2601

VIA ELECTRONIC SUBMISSION

Envestnet Yodlee response to the Australia Competition and Consumer Commission's (ACCC) draft rules that allow for accredited collecting third parties (intermediaries) to participate in the Consumer Data Right

Dear Commission Members,

Envestnet Yodlee ("Yodlee") welcomes this opportunity to provide feedback on the draft rules on intermediaries.

Yodlee is the leading global financial data aggregation platform provider, with twenty years in the industry, and ten years in Australia. Yodlee provides consumer-permissioned account aggregation capabilities with hosted solutions and commercial APIs on a business-to-business basis to customers around the world, including within Australia, that include traditional financial institutions of all sizes as well as financial technology companies. These customers offer data from Yodlee's platform to millions of retail consumers in Australia through the customer's own financial wellness solutions, which provide tools for consumers to track, manage, and improve their financial health across a host of different banks and financial institutions, as well as through platforms that provide financial advice and lending solutions.

We believe there are four key areas that need further review:

1. Meaningful adoption of Open Banking by consumers is not sustainable without a well-defined and operating accredited role for existing and new Intermediaries.
2. Looking at the current commercially managed ecosystem, it is clear that a "one size fits all" approach to intermediary accreditation will hinder innovation, consumer protection and CDR Rule's enforcement.
3. There is further differentiation needed between Outsourced Service Providers and Intermediaries to flexibly support existing and new engagement models and use cases while providing appropriate consumer protections and CDR Rule's enforcement.
4. Support of screen scraping and CDR API access/use, must co-exist as long as there is the current limited scope of "consumer data" available under CDR to data recipients from data holders.

Importance of Intermediaries

When the ACCC launched the Consumer Data Right (CDR) in November 2017 the goal was to "give consumers greater access to, and control over, their data"[1]. The CDR aims to empower consumers to

[1] ACCC Consumer Data Right

compare and switch between products and services, and to encourage competition between banks and service providers, all leading to improved financial wellbeing for Australia's citizens and greater innovation in the sector. Intermediaries such as Yodlee are currently fulfilling that role using commercial contracts in the absence of regulations. Ongoing support of intermediaries' critical role in the ecosystem is essential to ensure that consumers depending on the benefits of current solutions are not harmed and that the innovation solutions in the market, offered by incumbents and new entrants, can flourish to achieve the goal of Open Banking.

As evidenced by this consultation, the ACCC recognises the prevalence and importance of intermediaries to collect data from data holders as they support the uptake of the CDR and the development of innovative new products and services in the formation of the CDR and its supporting rules. Yodlee firmly believes however that further delays in enablement of this definitive role that accommodates the many different recipients of data today will delay the ACCC CDR objective of maximum possible participation of providers in the CDR and their assistance to Australian consumers and businesses in the post-COVID-19 recovery.

Unrestricted Accreditation vs Tiering models

The current CDR Rules support of only an unrestricted undifferentiated accreditation model where the ADR/Principal ultimately has liability for all data does not encompass support of all organisations that currently access consumer data including those through scraping mechanisms.

There must be sensible risk-based provision for the full spectrum of CDR participants; be it a new market entrant such as a small Fintech comparison website or large ADI with mature risk management practices in place such as a bank or credit bureau. In the current unrestricted heavily regulated model, the requirements for ongoing compliance programs will disadvantage new market entrants who do not have access to funding and internal legal and risk resources required for initial accreditation and ongoing compliance.

Maintaining this initial model will create unnecessary complexity that will pave the way for a new compliance sub-sector to fill the middle ground. Taking advantage of smaller Fintech firms that cannot operate in the proposed unrestricted only environment and therefore will profit on the limited legal and risk resources and naivety of smaller companies who wish to utilise the opportunities created by CDR. These compliance companies will exist only for the purpose of adding another cost and process layer though claiming to fill the gap in an overly complex regulatory framework further ensuring lower uptake, high costs and reduced innovation in the sector.

This is not to say that the use of consumer data and the activities of participants in the CDR regime do not have inherent security and privacy risks and must be managed appropriately. In order to uphold these security practices and see systemic adoption of the CDR in Australia, Yodlee believes there needs to be a scalable tiered accreditation and participation model that allows as many as possible qualified entrants to gain access to CDR data otherwise the regulatory burden for potential ADRs will be materially impacted and create barriers of entrance into the scheme.

As indicated we understand that this is a stated objective of the ACCC CDR. To assist in facilitating this we would like to provide the ACCC with guidance supporting the ACCCs and CAP intent on how we feel this could function as described below

1. **"Provider" Governance Model**

This model sees a "Provider" hold full accreditation into the CDR including liability and access to consumer data on the Data Holders side. This is little different to existing arrangements currently in place with large credit bureaus such as Equifax. The Data Holder knows and trusts the Provider and in some ways the Provider, although having standard agreements across all DHs, has a direct relationship and shares their risk posture and accreditation credentials; both with the ACCC and Data Holders network. Under this model an entity whom is a client of the Provider (though a potential ADR) does not need to become an unrestricted level accredited ADR (as the liability rests with the Provider). From a regulatory perspective this allows for the regulator to have a single point of recourse rather than concern over chasing multiple parties for breaches and the like.

This is the current business practice in place at Yodlee today. We place requirements on our clients and they sign up to a "Client Governance Framework and Program". This model was built for our US open banking program and UK Open Banking agents. Clients, and prospective clients, must complete an online security questionnaire and provide evidence of the design and operating effectiveness of their risk, security and privacy controls that support their Yodlee-powered service(s). If our assessment determines that necessary controls are not present, or not designed and operating effectively, a remediation process is initiated to bring the client into compliance with Yodlee's requirements. As mentioned, full liability to the ecosystem is upheld by Yodlee, so it is in the best interest of Yodlee to ensure there are no "bad players".

The Provider, Yodlee, is responsible for and guarantees the compliance and security of the receipt, processing, use and any retention of consumer data by them and its clients who are covered by the "Client Governance Framework and Program". Meeting CDR and OAIC standards and guidelines using in effect the successful "Sponsored" tiered accreditation and multi-party participation models in place in not only other Open Banking Frameworks but the wider global Payments and financial services industry.

Yodlee's Enhanced Client Governance Program is part of our overall Risk Management Program and subject to audit and reporting requirements to Management, the Board of Directors Compliance & Information Security Committee, regulators with standing and data providers with whom we have contractual agreements.

We are very open to confidentially sharing the policies and protocols of this program in working with the ACCC CDR in order to arrive at a more scalable framework in Australia and would welcome the use of this model as a basis for a Provider only accredited governance framework. This will release the burden on Principals holding all assurances and liabilities plus the cumbersome and costly task of having to gain unrestricted level accreditation as it exists in draft currently.

2. **CAP arrangement – "Provider/Principal" Governance model**

This model mirrors the draft CAP arrangement proposed by the ACCC where both the Provider and Principal enter into dual accreditation and a Combined Accreditation Person arrangement is in place. Liability however is shared on a commercial basis managed contractually between the two parties and based on the unique circumstances of this arrangement (e.g. the consent receipt and management including consent dashboard may be outsourced to the Provider and therefore the provider holds liability for this in the contract shared with the Principal).

Within this model only one consent token/authorisation number is used and is at the discretion of the Principal and the Provider for the purpose of recourse in the event of a breach.

3. Outsourced Service Provider – "Principal" Governance model

This model seeks to clarify the ambiguity that exists now between Intermediaries and Outsourced Service Providers. This is a complete Software as a Service (SAAS) model. The OSP is not accredited and is simply a "pass through" of data. They cannot provide any service using the data, to anyone other than the "Principal" to whom it is contracted. They cannot hold the data as the data is subject to the Consumer Data Right legislation and therefore in holding this data the subject must be accredited. The Principal takes full liability for all aspects of the data and collects the data under their accreditation status. The OSP can only operate with an accredited ADR and not in their own right.

The differences between this model and that of the other above models is further discussed below

Intermediary and Outsourced Service Provider

We believe the current rules are not clear enough to distinguish the difference between Intermediaries and Outsourced Service Providers. This causes confusion where currently there are a growing number of SAAS providers in market with "CDR" solutions. These providers have built and are maintaining these solutions to sell to Data Holders, ADRs and future intermediaries with the intention of there being a "pass through" of data. However the rules are extremely ambiguous around OSPs.

Paragraph 1.10A 1 (b) states an OSP as *"the recipient will provide, to the discloser, goods or services using CDR data"* which is the exact wording used to describe the arrangements of the Provider under a CAP arrangement: *"provide goods or services to the principal using a customer's CDR data".* Both the OSP and the CAP Provider arrangement have the ADR in the centre under a written contract allowing the OSP or the Provider to provide goods and services using CDR data.

With this in mind it is unclear why a data intermediary would take on the regulatory obligations of unrestricted accreditation and CAP arrangements when it can deliver comparable services to the ADR as an Outsourced Service Provider. We understand that full liability rests with the Principal however many intermediaries would be grateful for relinquishing this obligation. We also understand that OSPs cannot collect data in their own right or use purposes (as they are not accredited) however it is assumed they can collect under their client/ADRs consent token. Ultimately it is this "collection" and their provision of a service that causes the most concern as by collecting and providing a value add to the data it is by default gaining access to the confidential and regulated consumer data.

The value in using organisations such as Yodlee who have the experience and depth of governance and security standards over data practices including bank grade due diligence, structured contractual arrangements and close monitoring of their clients is somewhat negated in this model. An OSP could in theory create their own internal data management practice with no security controls due to the fact they do not need to comply with the CDR and therefore breach the ADRs accredited status in the process due to poor business practices.

CDR data vs non-CDR data User experience

As the CDR aims to provide consumers greater access to their data it cannot be overlooked that not all data will be available and flow through an open API in the short term. We anticipate a period in which the two will need to co-exist until the full "long tail" of financial service providers are operating under the CDR in Australia. Until this is the case there will be a need for consumers to be able to access their data through scraping mechanisms. Whilst large organisations such as Yodlee employ the most advanced and secure scraping techniques it is the customer experience under the new CDR that will cause most concern.

We believe attention needs to be given to the user interface as the current UX guidelines do not take into account the need for consumers to access data through non open banking APIs. There needs to be standard practice and terminology plus a common approach to the consent management process. Yodlee welcomes a consistent user interface for both forms of aggregation that negates the need for separate "sign-ons" and division of data. By way of example the consent screen could provide reference to the data clusters available through non-CDR and CDR mechanisms but the user name and password process is the same.

Also providers of non-CDR data need to be informed of simple terms like common reference to "screen scraping" techniques and how the ACCC would like to if at all draw attention to this practice in the consent flow. Without this commonality, organisations like Yodlee will be forced to create their own terminology and non-CDR consent processes which will confuse the consumer experience more. Again, Yodlee are only too happy to consult and work with the ACCC on this topic and provide guidance based on our global view and experience in other Open Banking regimes.

In conclusion Yodlee believes that data ultimately belongs to the end consumer. That the consumer should be able to access their data through the most secure means possible in order to arrive at their final destination; be it access to finance, a comparison of interest rates or a view of how they spend their money. As a firm that has been enabling these outcomes for over two decades, across many continents and open banking frameworks, Yodlee supports the role of practical regulations and accreditation in developing this Open Banking framework. We appreciate this opportunity to provide comment on the drafting of the Intermediary rules and welcome further discourse on this topic, be it in a public forum or direct with our local Australian team.