31 January 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) *CDR Consultation on how best to facilitate participation of third party service providers*

Dear Commission Members,

Envestnet Yodlee ("Yodlee") welcomes this opportunity to provide its perspective in response to the ACCC's request for input regarding the facilitation of participation of third party service providers in the accredited Open Banking ecosystem. As a firm that has been enabling consumer financial wellness globally for two decades, Yodlee supports the role of practical regulations and accreditation in the developing Open Banking framework. Moreover, we appreciate the opportunity to respectfully provide input with regard to suggested improvements in the design of the existing open banking ecosystem to ensure consumers are both adequately protected and empowered as they utilize open banking-powered tools.

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.

In its request for input, the ACCC asks the following questions.

1. *If you intend to be an intermediary in the CDR regime, or intend to use an intermediary, please provide a description of the goods or services you intend to provide to accredited persons or to CDR consumers using an intermediary. Do you intend (or intend to use an intermediary) to only*

Yodlee.com T + 1 650 980 3600 F + 1 650 620 9577

Headquarters: USA 3600 Bridge Parkway, Redwood City, CA 94065

collect CDR data, or collect and use CDR data? What value or economic efficiencies do you consider that intermediaries can bring to the CDR regime and for consumers?

Yodlee intends to be both an intermediary for the services we provide to our institutional and commercial clients, as well as an ADR for the limited services we provide direct to consumer. To be clear, we view these roles as separate and distinct, though there is the potential for overlap given the current state of regulation (of which this consultation may address). In the traditional consumer – provider – aggregator – data source model, the aggregator's role to enable the provider with a single development experience (i.e. APIs) to access the full range of data sources available via the aggregator's platform. Yodlee does this today, connecting our 1,100 clients to over 21,000 global data sources, providing such access via screen-scraping, regulated API, commercial API and data upload. In this capacity, the aggregator's use of the CDR data is strictly to collect and make it available to the provider (i.e. ADR). However, effective aggregation, and therefore a key value, requires that the aggregator normalize the data into a common data schema for the providers, which Yodlee does and will continue to do. We also categorize the transaction data (e.g. deposit, card payment for food, direct debit for utility bill) as well as enrich the transaction data to make it more understandable by humans and algorithms. This categorization and enrichment is performed only for the provider with whom the consumer is engaged, as we don't maintain a single view of the customer across providers. Yodlee considers the extent of this processing out of the scope of an ADR and therefore does not currently require authorization; and requests the ACCC provide explicit guidance on the same.

An additional value the intermediary brings to the ecosystem, especially as a regulated role, is uplifting the end-to-end security posture. There can be no question that the activities of the intermediary have inherent security and privacy risks that, if unregulated, are the responsibility of the ADR to manage. If the ADR is an ADI or large commercial entity with an effective vendor risk management program, then this may suffice to satisfy the requirements. However, if the ADR is a new market entrant, they will likely not have the resources or experience to manage the intermediary. In Yodlee's experience, as a long-standing service provider to global financial institutions and innovative fintechs, this is indeed the case. In fact, to address this risk in the current commercially managed ecosystem, we put requirements on our client and assess their risk and security posture, rather than they us.

2. *How should intermediaries be provided for in the rules? In your response please provide your views on whether the rules should adopt either an outsourcing model or an accreditation model, or both and, if so, and in what circumstances each model should apply.*

Yodlee strongly recommends that intermediaries who access CDR data via the regulated interfaces be subject to accreditation focused on the security of the technical solution as well as effective risk management for security and operations considerations. APRA's CPS 220, 234 and 235 are good starting points to define the prescriptive controls of Consumer Data, as is PCI-DSS (extending it from cardholder data to Consumer Data).

As intermediaries vary in the approach, scale and value added services, a contractual outsourcing arrangement between the ADR and the intermediary is still a necessary control to ensure properly managed and aligned oversight. As both parties are accredited, prudent risk management should inspire the intermediary to conduct reciprocal oversight of the ADR, thereby strengthening the level of protection for the consumers and ultimately the ecosystem. Yodlee already does this as part of a global risk management program, especially when dealing with non-accredited clients.

3. *What obligations should apply to intermediaries? For example, you may wish to provide comment on:*
    a. *if intermediaries are regulated under an accreditation model, the criteria for accreditation and whether they should be the same or different to the criteria that apply to the current 'unrestricted' level, and the extent to which intermediaries should be responsible for complying with the existing rules or data standards;*
    b. *if intermediaries are regulated under an outsourcing model, the extent to which contractual obligations should be regulated between accredited persons and intermediaries;*
    c. *if the obligations should differ depending on the nature of the service being provided by the intermediary.*

Yodlee recommends that intermediaries be obliged to follow all requirements, at the unrestricted level, for the safeguarding and governance of those aspects of the customer experience for which they are responsible or participate. Specifically, obligations for *fit and proper person, information security* and *insurance*. For example, all intermediaries should follow the data standard and supporting security requirements for the conduct of their staff and vendors; the security posture of their system assets that access, process and store consumer data; program to assess, detect, prevent and respond to security events; and regular assessments of the design and operating effectiveness of these control programs.

Depending on the value-add services provided to the intermediaries clients', they may also qualify for obligations for dispute resolution as well as qualify for requirements of other regulations and standards, such as for credit underwriting, payment card (i.e. PCI) etc.

4. *How should the use of intermediaries be made transparent to consumers? For example, you may wish to comment on requirements relating to consumer notification and consent.*

Yodlee recommends that disclosure regarding the use of intermediaries is required content in the ADR's customer terms and associated privacy notice. Given the commercial nature of the ecosystem, there is typically no practical way for a consumer to work with an ADR and not their designated intermediary so separate consent is not warranted.

5. *How should the rules permit the disclosure of CDR data between accredited persons? For example, you may wish to comment on requirements relating to consumer consent, notification and deletion of redundant data, as well as any rules or data standards that should be met.*

Consumers are best served with personalized services that respond to their particular needs with financial products and services designed to address their particular situation and needs. Accordingly, Yodlee commends the ACCC for this consideration in its consultation.

As is contemplated in the next question, tiered accreditation allows participants to focus regulated activities on just those related to their role and engagement with consumers' CDR data. For example, an accredited person that only receives de-identified CDR data from another unrestricted ADR for the purpose of consolidation and scoring by the primary ADR carries a different risk profile than one that processes the full set of raw data.

Yodlee recommends that the interests of the ecosystem and the protection of consumers is best served when all participates that interact with CDR data are accredited persons at a level appropriate to their participation and risk. All participants should be disclosed to the consumer and be required to follow the principled requirements of the Rule, such as data minimization, safeguarding and adherence to consent.

6. Should the creation of rules for intermediaries also facilitate lower tiers of accreditation? If so, how should the criteria and obligations of new tiers of accreditation differ from the current 'unrestricted' accreditation level, and what is the appropriate liability framework where an accredited intermediary is used?

The nature of the roles an accredited person may play in the provision of services to the consumer should be considered as the ACCC crafts a reasonable number of tiered accreditation levels, as well as inherent risk considerations for the liability framework such as volumes and types of CDR data accessed/processed.

Existing levels of accreditation should be considered in this framework for firms that also fall under APRA, ASIC or other regulatory regime, as well as ISO27001, PCI or applicable industry standards.

In undergoing an accreditation process, a set time period should be supported by the ACCC where appropriate internal resources are allocated to facilitate and expedite the process of accreditation. This would also permit new market entrants to qualify at the entry tier and move up the accreditation ladder as their business, and inherent risk posture, grows.

7. *If the ACCC amends the rules to allow disclosure from accredited persons to nonaccredited third parties and you intend to: a. receive CDR data as a non-accredited third party, please explain the goods or services you intend to provide, the purposes for which you propose to receive CDR data, and how this may benefit consumers; b. be an accredited person who discloses CDR data to non-accredited third parties, please explain the intended goods or services you intend to provide and how they may benefit consumers.*

Amendment of the rules to allow Yodlee as an ADR to provide CDR data to our clients who are unaccredited (b) will allow Yodlee to operate our commercial ecosystem "as is", with reasonable uplifts in the requirements we also flow down to our clients to comply with current regulations, standards and consumer protection standards. These services use the consumers own financial data for personalized engagement to help that consumer improve their financial wellbeing across the full spectrum of saving, spending, borrowing, planning and protection.

8. *What types of non-accredited third parties should be permitted to receive CDR data? Why is it appropriate for those types of third parties to be able to receive CDR data without being accredited?*

If amendment is made to permit non-accredited third parties to receive CDR data, Yodlee recommends there are key criteria that must be met for provider use case, amount and type of CDR data provided and the commercial contract. For example, Yodlee operates a tiered client governance program that allows new market entrants to test and learn with their own production financial data, then grow in size and scope with corresponding increases in the rigor of contractually required controls and governance. This model balances effective risk management with the needs of innovation, market safety and consumer protection.

9. *What privacy and consumer protections should apply where CDR data will be disclosed by an accredited person to a non-accredited third party? 10. What degree of transparency for CDR consumers should be required where an accredited person discloses CDR data to a non-accredited third party? For example, are there particular consent and notification obligations that should apply?*

Yodlee recommends that all privacy and consumer protection standards apply to the processing of CDR data whether the party is accredited or not, as it does now in the current ecosystem. The

consumer will likely engage with the non-accredited party with commercial terms that should disclose its accreditation status, the accredited provider with whom it is engaged and the required consents.

Yodlee would welcome the opportunity to discuss its perspective on how best to enable intermediaries as accredited persons in the Open Banking ecosystem.

Sincerely,

Brian J. Costello

Brian J. Costello, VP Data Strategy