

:86 400

SUBMISSION PAPER:

Recommendations from 86 400 Technology Pty Ltd on how to best facilitate participation of third-party service providers

January 2020

Overview -

- 1. The ACCC needs to quash anti-competitive behaviour and misinformation campaigns by the incumbent institutions. If they do not, Open Banking will not realise its potential, and consumers will be negatively impacted**
- 2. Intermediaries can accelerate and improve the CDR regime, and as such should be accredited accordingly**
- 3. Open banking and data sharing should be an opt-in model for a specific purpose, and the ACCC should ensure users are fully aware of the positive impact of the regime**

86 400 welcomes the opportunity to respond to the ACCC consultation paper which seeks to address the participation by third-party service providers within the Consumer Data Right (CDR) environment.

86 400 is in support of intermediary service providers and believes the full value of CDR will not be reached and the process slowed down by the current rules that rely on the consumer needing to register and renew their consent with original data holder. The ultimate cost being worn by consumers in the form of less competition and higher cost financial products.

While each individual question has been accorded a detailed response below, it is first appropriate that we share an outline of the centrality which 86 400 has accorded to CDR, within its core business model and in support of its customer needs.

86 400 has been at the forefront of championing customer access to their financial data, in order to help customers take control of their money and better manage their affairs. To this end, the bank has - from inception - enabled customers to link multiple accounts with other banking institutions within the 86 400 app. Using aggregation technology, users are able to see transactions made from 86 400 accounts along with transactions made across the totality of their financial spectrum. This facility has been offered on an optional basis and entirely without charge. Customers can choose to link all of their accounts, some of them or none of them and along the way they can also change their selections adding or removing as they see fit. Choice is imperative.

We have found that the functionality supported by 86 400 has been greatly valued by customers who appreciate the ability to manage their money through a single point of access using common navigation, rather than by requiring multiple logins. This capability has helped customers to track down individual payments much more easily than would otherwise have been possible and has enabled them to make better financial decisions.

We have further overlaid a regime of alerts to flag bills or payments that will fall due in the near future based upon past activity patterns across all linked accounts selected. This has helped customers to make bill payments on time and has consequently meant that late fees are minimised or avoided altogether. In addition, it has allowed customers the opportunity to cease services that they no longer require before renewal payments are levied. Amongst the many examples of the benefits that have been experienced, we are aware of customers cancelling gym memberships or subscriptions that they no longer use.

The read access to relevant and accurate personal financial data, in a timely and convenient fashion is the pre-eminent *raison d'être* behind the Consumer Data Right concept. It is therefore extremely disappointing that some institutions have actively and knowingly discouraged their customers from receiving the benefits that the embryonic framework is specifically designed to facilitate.

Ahead of the roll out of Open Banking, based on the European model, we have worked with Yodlee (part of the Envestnet group) to support our personal financial dashboard concept using their aggregation (“screen-scraping”) approach.

Yodlee operates globally in providing secure aggregation services to over 1,000 institutions including 15 of the top 20 U.S. banks. The approach allows read-only access to account information held with different institutions consistent with the CDR model. This data accessed is subject to 256-bit encryption standards both in transit and at rest. Log in credentials are not available to the recipient institution nor is it possible for any transactions to be carried out through the Yodlee mechanism.

Secure storage of log-in details is a necessary prerequisite for this functionality to be made available and this is specifically accommodated within the ePayments Code 2011 (S12.3).

Regrettably some institutions have actively discouraged their customers from accessing their own data by suggesting they are in breach of their account terms if they share their log in details with an aggregation service provider. These institutions have identified when aggregators such as Yodlee have successfully accessed data and frequently responded by telling customers that their security details have been compromised and that they should immediately change their passwords. The intent of this response is in order to defeat the aggregation service from continuing to access account information.

This is anti-competitive behaviour, is extremely misleading to customers and blatantly contrary to the principles espoused within Consumer Data Rights narrative.

86 400 uses a similar aggregation service in support of mortgage applications initiated by customers such that their full income and expenses can be quickly, accurately and easily ascertained, verified and appropriately classified. This approach allows an extremely convenient and accurate summary to be compiled to assist customers in assessing the affordability of a proposed facility. The convenience value for customers, faced with the alternative of manually compiling or estimating expenditures over a vast array of categories, is very significant.

As a leading advocate of responsible lending, this approach ensures that 86 400 has a fully detailed, robust and reliable data set against which to assess the ability of customers to afford mortgage payments under a range of different scenarios. This mitigates the risk of committing them to a facility that they might struggle to support in the future. Given that some expenditure and indeed some classes of income may arise only on an annual basis (such as bonuses or

holidays) we have sought to secure a full 12-month transaction history to augment the accuracy of our affordability algorithms. A number of institutions have knowingly and deliberately prevented access to customer data by our chosen aggregator or else have limited the quantum of customer data shared, often capping this at a few weeks or months of transactions.

Once again, we see this approach as both anti-competitive and contrary to the underlying CDR principles.

Customers should be able to access all their data in the manner of their choosing.

86 400 would be pleased to meet with ACCC representatives to expand upon our experiences in facilitating aggregation services if this would be useful.

Turning to the specific aspects raised in the consultation process we are pleased to address these below:

- 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 collect CDR data, or collect and use CDR data? What value or economic efficiencies do you consider that Consultation on the expansion of the Consumer Data Right rules for intermediaries can bring to the CDR regime and for consumers?**

86 400 expects to use CDR intermediaries (such as Yodlee) in the near term and ultimately to operate as an (ADI) intermediary itself. We anticipate a period during which traditional aggregation (“screen scraping”) services will operate in parallel with emergent technology in order to effectively access the full array of financial services providers operating within Australia. In due course we anticipate providing White Label services to third parties unable to economically access CDR data in their own right. The intent is to allow our customers (and customers using our technology through a White Label agreement) to be able to take control of their finances by having access to their full financial dashboard.

We expect that rules for intermediaries will allow for minimum technical specifications to be established and appropriate independent attestations to be established such that complying intermediaries will be allowed restricted access to customer data held by all participating institutions. We further expect that participating institutions will not be allowed to contact their customers, who have chosen to provide eligible intermediary access to a third party, with the intention of discouraging or denying them that access.

We are acutely aware that some large financial institutions may see little benefit in supporting CDR as they feel that the customer data they hold provides competitive advantage that they are reluctant to surrender. This is likely to cause them to slow down or otherwise inhibit progress initiatives in overcoming what is currently an unequal operating environment. By encouraging consultation and specifically facilitating intermediaries, we expect that this competitive disincentive can be called out early and bodies such as the ACCC might more effectively hold these institutions to account and force them to honour agreed timetables.

One of the benefits of the intermediary model is that dedicated intermediary institutions can develop sophisticated controls and heightened operational reliability whilst continuing to invest in the CDR ecosystem. At the same time smaller (consuming) institutions can focus their resources on a subset of the ecosystem. The ultimate benefits will be in the form of more choice, better services and lower costs for customers.

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.

We can see virtue in both outsourcing and accreditation models and in principle have no strong preference for one model over another. In practice we expect that an accreditation model may be simpler and faster to implement and as such this might be a more effective mechanism for supporting a rapid transition to a CDR environment.

An accreditation model would call for:

- a) Minimum standards (including redundancy) to be detailed
- b) Independent competent accreditation agents to be appointed and
- c) A centrally maintained register of such accreditations to be maintained that can be accessed by all participants

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.

We would expect that the standard for intermediaries under an accreditation model should mirror those for the current "unrestricted" level. An intermediary should be required to support current data standards but only to the extent that the data shared with them is compliant in the first place. There should be no higher obligation placed upon an intermediary than the primary data holder and no obligation to remedy failings in that data unless those failings were generated by the intermediary.

The introduction of an Intended Purpose approach would ensure that an individual customer consent could be effectively limited (for example in support of a mortgage application) without needing to be repeatedly provided for different ultimate users of the data (if for example a proposed lender is not able to provide a mortgage facility).

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.

Consent models breakdown when the frequency with which consent needs to be re-established or refreshed is unduly onerous. We would expect that transparent notification and ongoing consent could be provided for at the time of initial subscription to a product or service and (absent fundamental changes to the make-up of that service) the consent given should be deemed to be enduring.

Repeated and unnecessary refreshment of consents will likely bring the entire service into disrepute.

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.

Data should only be shared between accredited persons with the express consent of the customer involved and should be an opt-in model. Where an intermediary is acting on behalf of an accredited institution the authorisation of access should apply both to the accredited entity and the intermediary acting.

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?

We consider that any value to be gathered from tiered access would be less than the cost of administering a more complex regime and as such our preference would be for a single access approach.

7. If the ACCC amends the rules to allow disclosure from accredited persons to non-accredited 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;

We would expect to be an accredited third party. The following comment is offered in the interests of providing clarity.

Where a customer is seeking to refinance a loan, they would prefer to provide CDR consent once, even if the underlying data might ultimately be provided to multiple prospective lenders by a broker. Clearly this would be administratively less burdensome, faster and more cost effective. This presupposes the adoption of an "intended use" construct. The mortgage brokerage model would likely involve or call for provision of data to non-accredited third parties.

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.

86 400 Technology Pty Ltd (not an ADI but part of a Group containing an ADI) expects to act as a data recipient on behalf of other ADIs. In supporting other ADIs through the provision of similar insights and aggregated dashboards as are already available through the 86 400 app, we expect to facilitate enhanced customer understanding at a lower overall cost of delivery than would otherwise be feasible for each subscribing institution.

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?

We expect that some form of basic accreditation will be necessary for all data recipients in support of the intended use.

The technical implementation that supports the provision of data between an accredited entity and client will likely be proprietary and would necessarily embrace provisions around the protection of that data.

9. What privacy and consumer protections should apply where CDR data will be disclosed by an accredited person to a non-accredited third party?

The consent provided by the customer to the accredited party should be for a specific purpose. The accredited party must respect the limits of the consent and only pass data to third parties consistent with the consent parameters and with an obligation attaching requiring the third party to protect the data.

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?

We believe the accredited party (intermediary), acting as a data holder, should be subject to an appropriate consent process before they supply data to third parties. However we do not believe the provision of such data to third parties should require the consent of the original data holders as this would create unnecessary friction in the process and dilute the consumer proposition. The accredited party's (being a direct participant in CDR) obligation to disclose the parties they have directly shared the data with should remain.

Illustrative Example to highlight the participants involved and their potential interplay

The current consent model requires the Accredited Data Holder to be involved in the granting of consent to a Data Recipient. The consent rules need to allow an Intermediary to use the consent provided by the Consumer to the Accredited Data Holder for a given **Purpose**. The Purpose could require the Intermediary to provide the Consumer Data to a party that is not visible within the CDR ecosystem.

The consent process is problematic and risks making the regime untenable.

It is difficult to see why an enduring authority exists when a customer establishes a Direct Debit facility (which entitles a counterparty to take money from their account), but an apparently higher standard of consent needs to apply if data is being shared and that consent needs to be refreshed regularly. If CDR is to be effective, then the consent model needs to change such that customers aren't called upon to provide consent for the same activity on multiple different occasions.

The Intermediary should be able to provide this data to the other Party without referring back to the Accredited Data Holder and forcing the Consumer to provide another consent. The consent should be provided by the Consumer to the Intermediary only.

To explain this further, consider the following Parties and use case:

- a) Sam York; a 32 year old applying for a loan
- b) Sam uses a broker to find the right mortgage
- c) Sam is a digital native and wants to use the services of HelpMeOut.com.au (HMO); a CDR intermediary
- d) Sam logs onto to the HMO site and requests all of Sam's banks (Bank A, Bank B and Bank C) to provide account and transaction details to HMO.
- e) HMO collects the transactions from all three banks, and uses proprietary algorithms to identify income and expenses, and categorises them using rules applicable to those lenders Sam nominates.
- f) Sam instructs HMO to send the results to Bank X and Lender Y to compete for the mortgage.
- g) Neither Bank X or Lender Y is visible within CDR to the original Data Holder (Banks A, B and C). Only Sam and HMO know where the data has been sent.
- h) HMO has a commercial arrangement with Bank X and Lender Y that prevents them using the data for any other purpose than assessing the loan, and if the loan is not settled, there is an obligation to remove the data from their systems.
- i) Sam can revoke consent with an original Data Holder (Banks A, B and/or C) at any time and should this occur HMO would remove the data it holds and advise Bank X and Lender Y to remove the data from their systems as the loan is not progressing using their service.

- j) However, Sam is really pleased with the service HMO has provided and decides to use them for another investment property. As they still hold Sam's consent, they can immediately retrieve data from Bank A, B and C and forward to Bank X and Lender Y.
- k) 6 months later Sam is set to buy another property, and again goes to HMO. However, consent for Banks A, B and C has since expired

A mechanism needs to be applied to the consent process to allow Sam to provide consent for a period longer than 12 months (ideally in perpetuity), or else an automated process that allows HMO to renew the consent by acting as Sams agent; i.e. HMO has Sam's consent to extend the consent originally provided to Bank A, B and C.

The use case above could with only slight adjustment equally apply to an accountancy service or a financial advisory service or a myriad of different use cases each of which could legitimately need access to core data. This model exists today where banks offer third party access to customer's accounts via online banking platforms (with the customers consent) to individuals and companies and there is not a time limit applied to the access.

We contend that if the data truly belongs to the customer then they should be able to decide who else has access to it and banks should not be at the centre of that process, instead the customer should be at the centre. Once a customer has issued their instructions about who should have access to what data then that authority should suffice until such time as the customer revokes their instruction.

Yours Sincerely

Robert Bell

Chief Executive Officer

Brian Parker

Chief Information Officer