Australian Banking Association

07 February 2020

Mr Bruce Cooper
General Manager
Consumer Data Right Branch
Australian Competition and Consumer Commission
Level 2, 23 Marcus Clarke Street
Canberra ACT 2601
Via email: ACCC-CDR@accc.gov.au

Dear Bruce

ACCC CDR consultation on how to best facilitate participation of third party service providers

The Australian Banking Association (**ABA**) is pleased to make this submission in respect to the development of the rules governing operation of Third Party Service Providers (**TPSPs**) within the Consumer Data Right (**CDR**). With the active participation of its member banks in Australia, the ABA provides analysis, advice and advocacy for the banking industry and contributes to the development of public policy on banking and other financial services.

The ABA works with government, regulators and other stakeholders to improve public awareness and understanding of the industry's contribution to the economy and community. It strives to ensure Australia's banking customers continue to benefit from a stable, competitive and accessible banking industry.

The ABA supports the inclusion of TPSPs within the CDR regime. TPSPs could play an important role in the efficient and cost-effective provision of services to consumers. The entry of TPSPs, with appropriate governance and consumer protections, will enable the development of a richer and more vibrant ecosystem.

There is significant diversity in the business models, services and arrangements of TPSPs. The diversity of the business models of TPSPs can range from sophisticated software and data service providers through to individual accountants and financial planners. Given this complexity, the ABA believes that the ACCC needs to consider a number of principles to guide their development of the rules relating to TPSPs. The ABA has developed principles (attached) which will assist the ACCC in developing the consultation version of appropriate TPSP rules for the CDR regime.

At the core of these principles, is the ABA view consumers' data should not be less protected by the use of TPSPs than in the case of data held by accredited data recipients **(ADR)**.

As a key stone of the principles the ABA recommends an accreditation model for TPSPs that collect, hold or transmit CDR data, as opposed to an outsourced service provider model. This will ensure appropriate governance over the collection and use of CDR data as well as ongoing assurance that consumer protections, especially in relation to privacy and data security, are being met.

In the context of TPSPs, the ABA believes outsourcing arrangements between private entities will be insufficient to ensure adherence to the appropriate privacy and security requirements for CDR data as outsourcing arrangements cannot replicate the data governance of the CDR regime. An unregulated outsourcing model in the CDR regime is likely to: promote poor behaviours, reduce the level of accountability and therefore trust in the ecosystem; and make it difficult for the ACCC to enforce compliance. An accreditation model could also introduce overall efficiencies in the ecosystem. By allowing ADRs to select and use services from a range of accredited providers.

There may be various options for how TPSPs are accredited under the CDR however the primary goal must be to ensure that consumer trust and confidence in the regime maintained by preserving the existing consumer protection mechanisms in the CDR framework.

The ABA highlights three additional recommendations for consideration by the ACCC in its formulation of the rules under which TPSPs will operate within the CDR. First, banking data concerns financial data, it is important that any changes to the CDR in order to accommodate TPSPs does not introduce any systemic risk in the Australian financial and payments system. The ABA recommends that both the Reserve Bank of Australia **(RBA)** and the Australian Prudential Regulation Authority **(APRA)** be consulted on the potential systematic risks that TPSPs could create in the banking and payment systems.

Further, the ABA considers that there needs to be a clear distinction between an 'outsource provider' and TPSPs. This is especially pertinent in the case of Data Holders where the use of outsource providers (e.g.: cloud services provider) pertains to banking data in its pre-CDR form and the operations of the ADI is subject to the security standards and requirements of APRA (for example CPS 234).

Finally, the ABA recommends that there should be consideration regarding when the rules for TPSPs would come into effect. This is especially pertinent if those rules will result in changes to the rules and standards applicable to the existing CDR implementations by Data Holders and/or ADRs. It is unlikely that further changes to the rules and standards can be accommodated for the July and November launch phases of Open Banking.

As mentioned earlier, attached are the principles that the ABA believes the ACCC should take into account when developing the consultation version of the TPSP rules. Thank you for the opportunity to contribute to the development of the CDR. The ABA would be pleased to respond to any questions arising from this submission.

Kind Regards

Emma Penzo

Policy Director

Attachment:

Australian Banking Association

Principles for the development of rules in the CDR framework

TPSPs will perform many and disparate functions involving CDR data which, for example, may include use (including read access to the data), analysis, aggregation, transfer or transmit, and holding. Additionally, TPSPs may provide CDR specific related services such as consent management services. Collectively, these activities will be referred to as '**data management**'.

The ABA recommends that the following principles be considered as foundational in developing the rules for TPSPs in the data management services in the CDR:

1) **Consumer consent** – Data management should not take place without meaningful and informed consumer consent. To the extent relevant, and separate to the existing structures regarding outsourcing service providers, this means:
   a) the consumer must have ***full transparency*** regarding the use of TPSPs, and
   b) the consumer must ***provide consent*** for that data management to take place, and
   c) the rules should ***not permit on-sharing*** of the data which is outside of the original consumer consent.
2) **CDR data to be contained** – Except as already contemplated by the Act and Riles, CDR data should remain within the CDR ecosystem. The rules should not create an opportunity for the use of TPSPs' data management services to be undertaken by entities which are not subject to the CDR.
3) **Uniform security and privacy standards** –There should be no 'weak links' in the data management process. All TPSPs will be required to adhere to the security and privacy requirements applicable to the data management services it has been contracted to undertake under the CDR. For example, data transmission to/from TPSPs must be equivalent, in terms of security and privacy protections, to the data transfer requirements for transfers between the Data Holder and Accredited Data Recipient (ADR).
4) **TPSPs to be accredited –** TPSPs data management arrangements will vary. They may assist in the collection of CDR data or offer end-to-end services that collect and use CDR data. In either scenario, TPSPs must be accredited to ensure appropriate handling and use of consumer data. Different accreditation obligations may be useful to distinguish between the different risk profiles associated with different activities, however there should be no relaxing of obligations concerning security, privacy and consumer consent.
5) **Clear accountability** - Liability and accountability for resolving consumer complaints must be clear to participants and consumers where TPSPs are used in data management services. The ADR, as the entity with the direct relationship with the consumer, must carry primary responsibility in the event of any issues arising in the management of a consumer's data. This includes responding to consumer complaints and responding to regulator inquiries. Liability and accountability for resolving consumer complaints must be clear to participants and consumers where TPSPs are used in data management services. It must not be unduly onerous for a participant or consumer to seek remedies where multiple data recipients are involved in the chain of data collection and use.
6) **Clear distinction between ADR and TPSP roles –** It must be clear when an entity should be accredited as a TPSP or as an ADR. As an entity's activities may change over time, a review of the appropriate classification must be considered as part of the ongoing accreditation process. For example, where the operations of a TPSP evolve to become consumer facing and consumer serving, involving direct interaction with the consumer, they must become an ADR.
7) **Clear delineation between CDR data and non-CDR data** – The rules should not inadvertently capture data sharing arrangements between ADR and TPSPs or Data Holders and TPSPs which exist outside of the CDR.