Australian Banking Association

29 July 2020

Jodi Ross
Executive Director, Policy
Consumer Data Right Branch
Australian Competition & Consumer Commission

by email: ACCC-CDR@accc.gov.au

Dear Jodi

CDR Rules consultation Combined Accredited Persons Arrangements

The Australian Banking Association (ABA) makes this submission in respect to the CDR Rules consultation on the Combined Accredited Persons (CAP) arrangements.

Background: ACCC's CAP arrangements workshop

The ABA thanks the ACCC for the CAP arrangements workshop which it hosted on 14 July.

Take away points from that workshop were (i) that there was a legislative impediment the full range of Outsourced Service Provider (OSP) arrangements becoming fully operational as envisaged in Rule1.10. This is due to the OAIC advise that only accredited persons can have access to CDR data directly from a data holder (noting all banks and Data Recipients may already utilise OSPs to some extent within their technology platforms). (ii) That the ACCC was in the process of working through the legislative impediment (iii) That the CAP arrangement model was developed as a model by which data sharing, where an entity other than the Principal can have access to a consumer's CDR data directly from a data holder, could take place.

This submission is made on the basis that the Rules which will govern the 'simple' CAP arrangement, as anticipated in the draft Rule1.10A, need to be thought of in the context of an extensive model. Therefore, the Rules need to be scalable to the complex environment to avoid future reworking of Rules, standards, processes, and commercial arrangements amongst participants.

Key points and recommendations

The main instruments of the CDR, the Rules and the standards, do not capture the significant underlying complexity in implementation and ongoing operations of the CDR. The ABA strongly encourages the ACCC to develop detailed explanatory documentation to accompany the Rules which will act as an interpretive bridge from which the standards and the business processes of the CDR participants can be developed. In the case of the CAP arrangement, the documentation would include detailed worked out examples of scenarios for CAP arrangements which incorporate at a minimum the issues raised in the annexure.

Depending on the standards implementation, the CAP arrangement rule is expected to introduce significant complexity to the builds of the Data Holders. The introduction of intermediaries will require a rethink of consent, security, and customer experience (CX) guidelines. The ABA suggests that

additional to the detailed explanatory documentation, the draft standards need to be developed in draft, prior to finalising the Rules.

The annexure provides detailed feedback to the draft Rule10A. Based on that feedback, the ABA believes that a longer and more detailed consultation process is required for the CAP arrangement rule. The ABA would be concerned if the ACCC is planning to finalise and oblige implementation the CAP arrangement rule before the full implementation of the initial deployment of Open Banking across all ADIs is complete, especially in the event where Rule 1.10A will require build effort for the data holders. Implementation of this rule will also need to include adequate build time is factored into the developments of the non-initial Data Holders (non-major banks and other ADIs).

About the ABA

The ABA advocates for a strong, competitive, and innovative banking industry that delivers excellent and equitable outcomes for customers.

We promote and encourage policies that improve banking services for all Australians, through advocacy, research, policy expertise and thought leadership.

Please do contact me if you wish to discuss any aspect of this submission.

Kind regards

[redacted]

Emma Penzo
Policy Director
[redacted]

Australian Banking Association

Annexure: CDR Rules consultation Combined Accredited Persons Arrangements

1. Clarification of CAP arrangements

The ABA believes that the CAP arrangement rule should consider complex CAP arrangements. The following exemplifies the added complexity from CAP arrangements in the scaled state and highlights two issues for noting.

First, per *figure 1*, in the CAP arrangement model CDR data remains wholly within the CDR ecosystem[1], under the OSP model, the data is permitted to exit the ecosystem as it is reliant entirely on contractual arrangements between parties to ensure that the CDR Rules and standards are maintained.

The functional distinction between the CAP arrangement Model (Rule 1.10A) and the OSP model (Rule 1.10) has not been made clear in the Rules. If the key difference in the CAP arrangement is that the Provider will obtain or provide a service that relates to the collection or display of data for the consumer for the purpose of consumer sharing, then this needs to be articulated in the Rules.

The ABA recommends the Rules (or the explanatory documentation) make clear the commercial or functional distinction between an OSP and a Provider

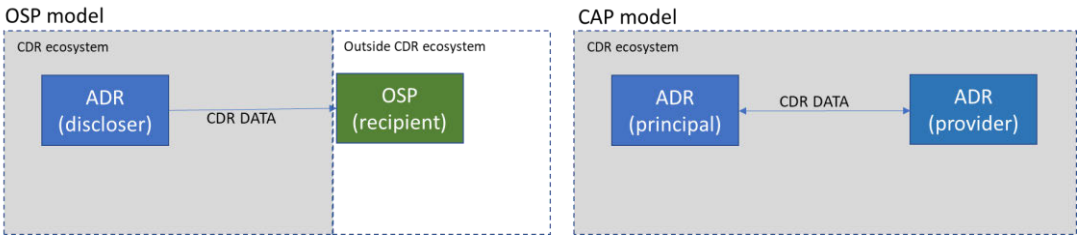

Figure 1

Second, the CAP arrangements have the potential to become significantly complex. The draft Rule 1.10A does not anticipate the complexity which will arise in respect to data flows under such arrangements. Although the ACCC noted at the Workshop that the intention of Rule1.10A was to cater to one Provider and one Principle as a CAP arrangement unit, the commercial opportunity for expansion of that model to cater to more than two entities in a CAP arrangement will be pressing. Figure 2 represents a moderately complex CAP arrangement model will likely develop as the CDR increases functionality, data availability and the number of participants in the ecosystem.

[1] Where the ecosystem is defined as that which bounds CDR data within accredited entities (both data holder and accredited data receiver).

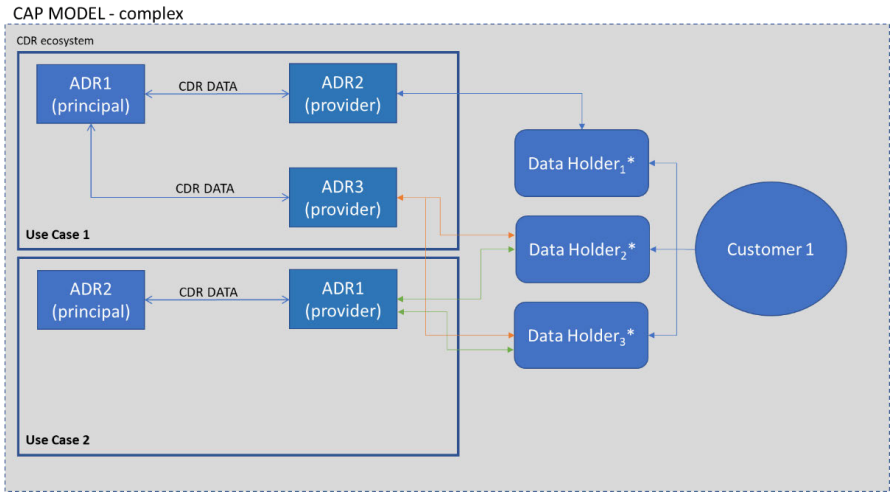

Figure 2: Complex CAP arrangement model

To 'enliven' the model depicted in figure 2, the following commercial example is put forward.

The participant profiles:

- ADR 1 runs a general financial advice business which helps consumers identify the banking products most suited to their financial behaviours
- ADR 2 is an app developer and has expertise in the analysis of mobile phone usage patterns to predict consumer future activities.
- ADR 3 has AI expertise and has developed a tool which analyses consumer transaction patterns and makes predictions on the consumers future purchase behaviours.
- Data Holder (DH)1 is a Telco and DH2 and DH3 are ADIs.

Use Case 1: Seeks to provide insights to Customer 1 by combining the customer's mobile phone usage with their banking transaction data. ADR 1 acting as the Principal has engaged ADR 2 (Provider), which has expertise in telco data analysis to be its provider for Customer 1's mobile phone data. ADR 1 (Principal) has also engaged ADR 3 (Provider), an expert in financial data analysis, to be a Provider for Customer 1's transaction data. ADR 1 will manipulate both data sets to derive insights which it will present to Customer 1. To compile the data, ADR 2 will access data from the telco (DH), and ADR 3 will access data from two ADIs (DH).

Use Case 2: ADR2 has developed a smart digital wallet which provides enhanced payments capability to consumer. That is, rather than simply responding to a consumer request to process a payment, the wallet can affect consumer purchase behaviour at the point of sale. This wallet has the potential to significantly disrupt social marketing activities because in a digital marketplace, there is no 'shame' factor for a customer to abandon his shopping cart on the prompting of a 'voice' which reminds him of his 'higher' financial goals and current financial state. Due to the good working relationship with use case 1, ADR 2 launches use case 2. ADR 1 will provide its insights from use case 1.

The ABA recommends that the Rules (and explanatory documentation) anticipate for the complex CAP arrangement state so that the built solutions can be scalable.

Australian Banking Association

2. Definitions

Whilst the simple CAP arrangement model has been defined, its constituent entities have not been. This raises complexities and questions which require clarification. For example:

- Does 'Principal' have the same meaning as 'Accredited Data Recipient' and an 'Accredited Person'?
- Does an entity that is a 'Provider' have a lesser obligation for compliance even through it is also an Accredited Data Recipient?

The ABA recommends that 'Principal' and 'Provider' be defined terms in the CDR Rules.

3. Principal/Provider functional clarification

The interchangeable relationship under a CAP arrangement between the Principal and Provider has not been made sufficiently clear in draft Rule 1.10A(1). This in part is due to the lack of definition for the Principal and the Provider. If understood correctly, the effect of the CAP arrangement is such that the Provider can discharge the obligations of the Principal on behalf of the Principal. For example, if the Provider is collecting the data, obtaining consent, providing the good or service, then the Provider can also undertake the regulatory reporting as well as correct the data.

Subsection (1) needs to be broad so that it is clear that the Provider (subject to being authorised by the Principal) has the same rights and the same obligations as the Principal. That way, the CAP arrangement between the Principal and Provider will dictate which rights and obligations will be performed by the Principal and the Provider (but both are responsible under subsection (4)).

The ABA recommends that the ACCC consider the following drafting changes (bold and underlined) for draft Rule 1.10A(1):

Draft Rule 1.10A (1) (suggested amendments underlined in bold)
1.10 A Combined accredited person (CAP) arrangements (1) An accredited person (the *principal*) may enter into an arrangement with another accredited person (the *provider*) for the provider **to perform any or all functions and obligations of the principal in relation to CDR data on behalf of the principal, including do any of the following:** (a) collect a customer's CDR data from a data holder on behalf of the principal, including obtaining consents and making consumer data requests; (b) provide goods or services to the principal using a customer's CDR data collected on behalf of the principal or disclosed to the provider by the principal for that purpose. Example: The provider might undertake to collect a CDR consumer's CDR data from a data holder where the CDR consumer has given the principal a valid request to seek to collect that CDR data from the data holder. **Example: the provider might undertake to respond to correction requests.** Note: Because the CDR data is collected and used by the provider on behalf of the principal, the principal is an accredited data recipient of the CDR data, whether or not the data is actually received by it (see section 56AK of the Act).

4. Informed Consumer Consent

In the case of the basic and extended models as described in section 1, there is question regarding the consumer's ability to provide fully informed consent for CAP arrangements in the context of the consent flow. Rule 1.14(3)(i) and Rule 4.11(3)(i) introduces a requirement for the CAP arrangement to be disclosed as part of the consent flow. There is a significant volume of information which is mandated to be included in the consent flow via Rule 4.11(3)(i) which may make it complex for the consumer to comprehend and potentially impede the consumer's ability to provide informed consent.

Taking the example of use case 1 and use case 2 above, the question arises, what is the envisaged consent flow in these situations? There is a practical concern about how consent is captured and revoked when there are multiple ADRs. In this example, ADR3 is accessing data from the DH, how does the ACCC envisage the concept of 'on behalf of' operating from a technical perspective?

In a future case where the data is also stored by an OSP, additional consents will be required. What consent model is envisaged will be appropriate for the customer in this situation?

This example also highlights the requirement for each ADR to have a CDR Policy that is made available to the consumer. Therefore, the customer could be presented with three different polices (refer to section 9).

The ABA recommends leveraging CX guidelines consultation processes so that complex arrangements can be tested in advance such that the consumer has full transparency and understanding of the consents they provide.

5. Obligations

Draft Rule 1.10A(4) does not require the parties to a CAP arrangement to apportion responsibility for the discharge of obligations in respect of CDR Data, which may lead to confusion between the parties as to who is responsible for discharging an obligation. This confusion, in turn, would lead to poor consumer outcomes, and potentially compliance gaps. As contractual obligations of CAP arrangements will not be visible to regulators, these terms should be reviewable or auditable by the ACCC and depending on the service provided, the OAIC and ASIC (for example, in the case of mortgage advice provision ASIC's best interest duties may be invoked). Contractual arrangements between CAP arrangement participants should be reviewed regularly by the ACCC.

In addition to the CAP arrangement clearly spelling out whether the Principal or Provider will discharge an obligation, the Rules must impose an obligation on the Provider to comply with the specific Rules that correlate to the services being performed on behalf of the Principal. Those Rules should apply in addition to the Rules that apply to 'Accredited Persons.' It is noted that Providers will provide different services and there is a need to retain flexibility in compliance, but the ACCC could provide guidance on what Rules will have to be complied with by the Provider. The Principal should not be responsible for the Provider's compliance with Rules that apply to a specific service being performed by the Provider, otherwise the Provider will not be incentivised to comply as they will always be able to rely on the Principal.

Take the following example: A Principal is seeking to provide advice on appropriate mortgage products to its customers. It engages the Provider to provide analysis of a customers' income and expense patterns and in so doing provides estimates for appropriate borrowing floors and ceilings for the customer. The Principal uses that analysis as input in its own analysis as to which mortgage product is best suited to the customer. Based on this example, the Provider should be responsible for its analysis and recommendations on mortgage borrowing amounts.

Australian Banking Association

6. Liability

Draft Rule 1.10A(4)(b) only enforces the obligations on the Principal. For example, Rule 7.6(2A) provides that if CDR data is collected by or disclosed to a Provider in accordance with a CAP arrangement, any use or disclosure of that CDR data by the Provider (whether or not in accordance with the arrangement) is taken to have also been by the Principal. This position raises concerns around efficacy and fairness of the liability structure of the CAP arrangement, and access to redress by the Principal.

Efficacy and fairness of the proposed liability structure

The rationale for liability being on the Principal appears to be for the purposes of aligning with the liability requirements for outsourcing arrangements (as per p.4 of the explanatory statement). Whilst this might be seen to be appropriate because from the consumer's perspective the Principal is the brand/entity with which she is dealing, if in practice the Provider has been engaged because of its capacity to provide significant 'value add', the Provider should also be held to account for any breaches or misuse or unethical use of consumer data. The current drafting of Rule 1.10A negates any contributory responsibility the Provider has in such circumstances.

Therefore, it is not appropriate that the CAP arrangement liability mirrors the outsourcing arrangements. The underlying reason an ADR must remain liable for breaches by an OSP is that the OSP sits outside the CDR regulatory framework and is not required to become accredited. By mirroring that approach and making a Principal liable for the acts or omissions of the Provider where the Provider is accredited, the ACCC is mandating all the compliance risk sits with the Principal and relieves the Provider of any risk with respect to enforcement by the ACCC or OAIC under the regulatory framework. Accordingly, despite being accredited, the Provider has no fear of enforcement, and need only concern itself with potential recourse from the Principal. It introduces, in economic terms, a 'free rider' incentive for the Provider.

It is foreseeable that this liability structure will lead to outcomes that compromise the efficacy of the CAP arrangements. Two examples are: it may lead to Principals not engaging Providers due to the risks, leading to less new market entrants; the development of a realistic edge case which is a 'reverse' CAP arrangement where a commercially 'captured' Principal's business model is determined by the Provider.

Inadequate Redress

The draft Rule does not contemplate what redress will be available to a Principal against a Provider who is not meeting their obligations. Therefore, there is greater pressure on the Principal to have in place contractually negotiated robust liability provisions with the Provider to appropriately apportion liability based on the expertise and control of each party. For example, despite draft Rule 1.10A(4), the decision regarding whether redundant data is to be deleted or de-identified in accordance with Rule 4.17(1)(c) is to be made by the Principal (see Rule 7.12(1A)). From a practical perspective, there needs to be contractual arrangements between Principal and Provider such that the Provider is mandated to treat redundant data in accordance with the Principal's election and this will increase the barriers of entry using intermediaries.

The Principal should not be responsible for trying to negotiate into a CAP arrangement a liability package that appropriately and proportionally allocates liability that sits entirely on the Principal. Regardless of the negotiation power of the Principal, it is inappropriate where the Provider is accredited and has contributory responsibility.

The ABA recommends that the ACCC reconsider the liability structure of CAP arrangements. Providers should be held responsible for their services within the CAP arrangement. Further, the ABA recommends that the ACCC should stipulate conditions under which it would deregister a Provider but

permit the ongoing operation of the Principal. In the case where enforcement is to be taken against a Provider, the enforcement action should not extend to the Principal nor to the Principal's software or systems. Additionally, the ACCC should clarify the obligations and liability of parties in complex situations.

7. Dashboards

The combination of **Rule 1.14, Rule 1.10(3)(a), and Rule 7.4** (Subdivision 7.2.2) has been interpreted to mean that it is the Provider who must supply the customer dashboard.

The ABA suggests clarification as to which entity, if any, is mandated to provide the customer dashboard in a CAP arrangement.

8. Register standards and CDR standards impacts

Draft Rule 1.10A(1)(a) and (b) states that the Provider can act partially or completely on behalf of the Principal, including obtaining consents and making consumer data requests. From a system's build perspective this creates a 'break' in the current relationships as per the Register design. This raises the following questions (amongst others):

- How will such a requirement be implemented in respect to the Register design and the token exchange between DH and ADR.
- In a situation where a Principal ADR may offer two use cases to the same customer. Use Case 1 will be fulfilled by the Provider ADR and Use Case 2 will be fulfilled by the Principal ADR. Both use cases are to be offered to the same customer for CDR data which is held by the one DH. In this example, would the current Register design allow for such cases?
- Is the Provider permitted to manage the revocation process? This appears to be inferred by 1.10A(1)(a). If so, would a Provider/ADR need to have multiple revocation end points?
- What other changes to the CDR standards will be required (e.g. security, consent)?

The ABA recommends that the token exchanged between DH and ADR should enable the DH to identify when a Provider is collecting or receiving CDR Data, and to identify the Principal. This is required for cybersecurity, fraud detection, auditing, reporting, frontline enquiries from consumers etc.

Irrespective of whether there is an obligation to check the identities of all CAP arrangement participants, DHs must have the ability to record the details of both the Provider and the Principal ADR. For example, if a Provider is compromised and is collecting data on behalf of several ADRs, looking at the ADR data alone may not make the source of compromise clear. Additionally, if a DH detects a compromised Provider, it could have flow-on effects to several ADRs therefore identifying this early would be beneficial to the ecosystem.

The ABA strongly recommends that prior to the CAP arrangement rule being finalised a concurrent standards consultation process be undertaken to ensure that any changes to the standards (e.g. Register, security, consent) will be accommodated in the Rules.

9. Rule 4.11 and Privacy Safeguard 1

Rule 4.11.3.i.iv includes the Provider's CDR Policy. However, this raises the situation where there could be two policies provided to the consumer, that of the Principal's and the Provider's. Given the liability structure envisaged by the current drafting of the Rules, it would appear to be appropriate for the Principal's policy to persist.

Privacy Safeguard 1 will also become complex as both the Provider and Principal will be required to have policies. Clarity is required as to which the customer is to follow.

The ABA recommends that the dual policy situation be clarified to inform the consumer how she should proceed in the case of a dispute.

10. Rule 9.4 Reporting requirements

The reporting requirements in Rule 9.4 are silent on the Provider, therefore it is assumed that the obligation sits with the Principal. An alternative interpretation is that the Provider is also required to report, as the entity is also an ADR. It would be beneficial to clarify which party would be permitted to submit a regulatory report. The ABA assumes that procedures and data standards would need to allow for CAP arrangements if a third party (the Provider) conducted the reporting on behalf of a Principal.

The ABA recommends accreditation requirements and Rules specify responsible entity for regulatory reporting.

11. Rule 9.7 Audits by the Data Recipient Accreditor

The audit requirements in Rule 9.7 are silent on the Provider, therefore it is assumed that the obligation sits with the Principal. An alternative interpretation is that the Provider is also required to adhere to the audit requirements, as the entity is also an ADR.

The ABA recommends clarification in respect to the Provider's audit obligations.

12. Control Requirement 1 - Encryption in transit

The ABA notes that the term "*Description of minimum controls*" is broad and covers areas unrelated to encryption. The ABA suggests that "*Auditing data access and use*" and "*implementing processes to verify the identity of communications*" should be located in "Audit Logging and Monitoring" and "Access Security" respectively.

The ABA notes that "*Industry best practice*" is a subjective term and recommends that it should not be used in a prescriptive standard. The ABA suggests that entities bound by these Rules are referred to guidance provided by ACSC at this link..

13. Technical complexity

The brief assessment of the draft Rules undertaken by the industry points to a significant increase in complexity introduced by the CAP arrangement rule. Rework will need to be planned for the standards and therefore to the builds of Data Holders.

Bank technical experts highlight that the introduction of intermediaries will require a rethink of consent, security, and customer experience (CX) guidelines. At a more detailed level requirements such as those for Transaction ID Permanency, token binding to client certificate, token issuance, consent token decryption and arrangement id; will require assessment. Each of these require a consistent implementation at the software product level.

The ABA strongly suggests that additional to the detailed explanatory documentation, the draft standards (both DSB and Register) need to be developed concurrently to the draft Rule, and most certainly prior to finalising Rule 1.10A.

14. Other points

Complaints/Dispute resolution: The ABA queries whether a third party service provider (TPP) would fit into the external dispute resolution scheme requirement if the TPP became an ADR, and whether there would be any practical challenges around the processing of complaints data by the Principal in this case?

Corrections process and notification: The ABA recommends that the Rules specify the obligations of Providers.

Further guidance: The ABA requests the ACCC to provide specific use cases to inform thinking for the development of Rules and standards. Additionally, interpretive guidance through an explanatory document and use cases would be beneficial once the CDR obligation responsibility and liability from each party to the CAP arrangement is finalised.

15. Privacy impact assessment

15.1 CAP arrangements

The ABA supports the recommendations in the PIA regarding CAP arrangements and for the Rules to include more specificity for CAP arrangements around the obligations of the Provider and Principal ADRs particularly in relation to withdrawal of consumer consent and liability framework (see PIA, page 14 -16 and also item 22, PIA, page 30).

15.2 Collection of CDR Consumer Consent

The ABA agrees with the risk raised by Maddocks in relation to consumers being unaware who is collecting their data as a result of the Provider/Principal ADRs and CAP arrangements. The requirements in the Rules to disclose details about the Provider ADR will likely add to 'information overload' for consumers rather than add to the knowledge of the consumer (refer to PIA, page 18).

15.3 Data Holder to check credentials of Principal/Provider ADR prior to disclosure

Recommendation, item 11 (PIA, page 22) pushes the burden on the DH to check credentials of both the Principal and Provider ADR prior to disclosure. This adds an additional step for DHs and where the Register is not up to date this creates increased risk to the DH.

The ABA suggests that the onus to check credentials should be on Provider rather than DH.

15.4 Provider ADR discloses CDR Data to Principal ADR

The ABA supports the recommendation in item 21 (PIA, page 26) that the ACCC include in the legislative framework specific technical requirements to reduce the risks of CDR Data being sent to the incorrect ADR as a result of intermediaries.

15.5 Withdrawal or expiry of CDR consumer Authorisation

The ABA agrees with the risk highlighted in item 24 (PIA, page 32). There should be clarity in the Rules regarding notification of who is the Principal ADR and who is the Provider ADR and this should also be communicated to DHs.

15.6 Suspension, Revocation or Surrender of Accreditation

The ABA agrees with the risk highlighted in item 26 (PIA, page 34) in relation to previously-accredited data recipients (either the Provider ADR or the Principal ADR) continuing to use or disclose CDR Data and generally support the recommendation.

The ABA seeks clarity as to whether this is intended to also ensure that DHs are notified of a suspension. If not, such notification should be made to the DH.

Additionally, the ABA queries whether there should also be ability in the Rules for Principals to mandate deletion or de-identification of redundant data where a provider is no longer accredited.