Question	Question	Position / Comments
We welcome comments on the proposed timeline for the proposals referred to in the CDR Roadmap.	1	Like many participants, SDS requires many of the suggested changes to be made as soon as possible, that is we agree with the proposed timeline if anything would prefer it be done even quicker. However, this does need to be balanced with existing workloads and budgets which are already at bursting point. We feel the introduction of the extra levels of accreditation is critical to new participants entering the system and therefore, consumer adoption.
The proposed rules include three discrete kinds of restricted accreditation (i.e. separate affiliate, data enclave or limited data restrictions). We welcome views on this approach and whether it would provide sufficient flexibility for participants. In responding to this question, you may wish to consider whether, for example, restricted accreditation should instead be based on a level of accreditation that permits people to do a range of authorised activities.	2	We believe all suggested models are technically achievable and are risk appropriate. We have and continue to discuss accreditation levels with various FinTechs and have been able to match business cases with each level of accreditation. We do believe these levels will meet the required outcome of allowing new participants into the CDR regime while maintaining a balance between risk & cost of accreditation (and ongoing compliance).
We also welcome views on alternative risk-based restrictions that could apply to a lower level/s of accreditation, as envisaged by the Open Banking Report, including views on whether, and in what way, an approach based on volume (for example, volume of customers or customer records), could provide an appropriate basis for developing levels of accreditation	3	SISS suggests that the ACCC Registry recorded the scopes requested for each Accredited Person, as well as the subset of scopes that a Product under this Accredited Person requires. By having the register hold details of the scopes an ADR requires, it would allow Data Holders and CAP Providers to be able to ensure ADRs are only requesting the required scopes. This would also allow Accredited Persons to be graded based on risk, which could be used to set Accreditation requirements.
What are your views on the low to medium classification of risk for the data set out in Table 1?	4	Basic Bank Account Data – We agree this is low risk Detailed Bank Account Data We agree this is a medium risk Basic Customer Data – We agree this is low risk Bank Payee Data – We agree this is a medium risk with one caveat** Bank Regular Payments – We agree this is a medium risk with one caveat**

		** In regard to the payee & regular payments data we feel some of the details in these data set is actually more sensitive than say transaction data. For example, take a small business who uses their banks' payee function to pay their employee salary. This means the banking details of employees are disclosure to an ADR with the lowest level of accreditation. Similarly, access to scheduled payments is akin to giving access to transaction data. In combination with other datasets this level of detail could be used to reverse engineer a number of details or at least a close estimate. We note that one purpose for this level of accreditation could be something like a 'switching service', that is moving a consumer's primary transaction banking from one bank to another. Such a service would require access to all these details; however, a switching service is likely to be utilised by a data holder with a higher level of accreditation; therefore, access to this data is appropriate. We would suggest some consideration to two data scope levels for payees & schedule payments; basic and detailed and ADR with this restricted level of accreditation only be allowed access to the basic level of data where some details are either removed or masked.
Are the accreditation criteria that apply to a person accredited to the restricted accreditation level (limited data restriction) appropriate for that level?	5	Yes, we believe this level is appropriate and will fulfil the objective of encouraging more participants into the CDR ecosystem. We do feel any level of attestation provided should be provided by a representative with appropriate security professional, i.e. CISP etc. Should a participant not have their own appropriately qualified professional, then perhaps a requirement to engage with one or enter into a CAP arrangement.
Do you consider the restricted level (limited data restriction) would encourage participation in the CDR? What are the potential use cases that this level of accreditation would support, including use cases that would rely on the scope of data available under this level increasing as the CDR expands to cover new sectors beyond banking?	6	Yes, there are many known user cases for this model. We also feel there are many unknown user cases still to be thought of. Some examples of know business cases include (but not limited to) • Validation of a bank account, that is the account exists and who owns it • Validation of available funds before processing a payment, reducing dishonour fees, administration, consumer embarrassment and potential legal consequences for missed payments • Auditors performing compliance checks for any number of legal, taxation, administration or regulatory requirement • Could allow the next big “app” to access data in a proof of concept phase to get traction, investment & allow growth as they evolve into the higher levels of accreditation • Allows consented parties like financial counsellors, financial planners to become accredited and monitor their clients bank balance • This base level of accreditation may allow for comparator services to review the type of accounts to determine more applicable products and ultimately offer a ‘switching’ service

Do you consider the data enclave restriction would increase participation in the CDR? Where possible, please have regard to potential use cases in the banking sector and	7	Yes. Many participants only require some form of analysis run over a dataset to provide a verification, result or insight. Many may not want to collect the entire CDR dataset into their systems to run this analysis. Some participants wat to use enclave solutions to mindfully reduce their security footprint Potential business cases include (but not limited too) • Account Validation, allows a participant to validate existence and ownership of an account(s) • Lending Data set, in order to assess loan serviceability • Income Verification • SMSF Auditing – Balance check • Statutory Auditing – Balance Check • Spending & Budgeting analysis • Insurance payments • Ensure Superannuation transfers and payments • Validation of transactions
Should the combined accredited person (CAP) arrangement between an enclave provider and a restricted level person include additional requirements, for example, in relation to incident management between the parties?	8	Yes, we believe the written CAP arrangement should specify the roles and responsibilities around the various requirements. As principal recipient is the client-facing service we feel they are they hold the default responsibility. While we acknowledge the ACCC don't want to determine the text of a CAP arrangement, we do believe a list of minimum requirements that CAP should cover be developed. The list of minimum requirements would be documentation and agreement around requirements like • Incident management • Customer complaints • Dispute resolution • ACCC Reporting compliance
Should there be additional requirements under Part 1 of Schedule 2 for enclave providers in relation to the management of data enclaves?	9	Joint policy on the services provided by each under CAP arrangement and who is responsible & liable. The joint policy should include. • Services provided by each party • Disclosure to customers • Decoupling of the service • Obligations surviving post termination of the agreement
Do you consider the affiliate restriction level would increase participation in the CDR? Where possible, please have regard to	10	Yes, we believe this model is highly desirable as many future participants would like access to data in order to serve the consumer The primary reasons this model is desirable

potential use cases in the banking sector and future CDR sectors.		• Reduces cost to build • Reduces cost to maintain and comply • Improves speed to market • Allows for a natural progression through the levels of accreditation. That is an ADR can implement a proof of concept via the enclave level as they grow switch to an affiliate level and eventually become a full unrestricted level while still utilising a CAP or become unrestricted in their own right. • Allows participants to focus on their core service while utilising the technology & experience of data experts. For many participants, data may not be considered a core function, rather an 'extra' or 'addon' that is it improves their service offering but is not essential to it. • Allows participants to share technical, business and financial risk Note the enclave and affiliate levels of accreditation share many common reasons for using a CAP arrangement. These common reasons do not invalidate either accreditation level as each participant will have a different profile around the purpose for data, cost, risk, volume, delivery model, consumer profile and technical capacity. The profile of the participant will determine which accreditation level is most appropriate.
Should there be additional requirements under Part 1 of Schedule 2 for sponsors?	11	SISS believes that the requirements on sponsors (being all the required ADR controls) is applicable. Question for SDS: the main issue is 5.1.(D).6: "*The sponsor of an affiliate must take reasonable steps to ensure that the affiliate complies with its obligations as an accredited person.*" What are reasonable steps? Given our liability, if they are deemed non-compliant. We could ask for them to detail what is reasonable, but it might make the process more complex.
Where a sponsor and affiliate rely on a CAP arrangement, should the CAP arrangement include additional requirements, for example, in relation to incident management between the parties?	12	Under the CAP arrangement, we acknowledge the requirement for a consumer complaints process. We believe the primary requirement for this to be held by the principal as they are the consumer-facing service provider. Fundamentally all participants have access As the CAP arrangement is required to be a written document, we believe this document should include a reference to how the complaint process will be handled within the context of the CAP. We understand (and agree) that ACCC don't wish to specify the actual text of these arrangements, but we do believe that ACCC should specify that certain requirements are documented, and roles assigned.

The draft rules envisage that all of Schedule 2 will apply to an affiliate of a sponsor. However, depending on the relationship between the sponsor and the affiliate, there may be options to reduce the risk associated with this model which in turn could result in less controls being relevant for some affiliates. We are interested in views on whether a distinction could, or should, be made for different levels of access to data between sponsors and affiliates (some examples below), and, if so, what approach to assurance of the information security criterion may be appropriate. **Example level 1**: affiliate is able to obtain access to any CDR data collected by the accredited sponsor and all data is held and managed on the affiliate member's systems. **Example level 2:** affiliate is able to access all data sets but uses some of the sponsor's systems and applications to access or manage the data. **Example level 3**: affiliate obtains access to a limited amount of CDR data held by the sponsor, or entirely uses the accredited sponsor's systems and applications to access or manage the data	13	SDS would recommend that this also be driven by the scope and its associated risk, as an affiliate who is only getting Basic Bank Account Data carries a much lower risk than one who can access all scopes of data. Example Level 1 – if the affiliate is able to access any of the CDR Data the accredited sponsor, and if the scopes they can access includes the high risk scope(s) i.e. Detailed Transaction Data, then their accreditation should require that similar controls as applied to the sponsor be in place (as assessed by the sponsor). Lower control requirements could be considered for lower risk scopes. Example Level 2 – if the affiliate is able to access any of the CDR Data the accredited sponsor, and if the scopes they can access includes the high risk scope(s) i.e. Detailed Transaction Data, then their accreditation should require that similar controls as applied to the sponsor be in place (as assessed by the sponsor). Lower control requirements could be considered for lower risk scopes. Example Level 3 – if the affiliate is able to access any of the CDR Data the accredited sponsor, and if the scopes they can access includes the high risk scope(s) i.e. Detailed Transaction Data, then their accreditation should require that similar controls as applied to the sponsor be in place (as assessed by the sponsor). A higher number of lower control requirements could be considered for lower risk scopes.
We consider that in the case of a CAP arrangement, it is appropriate for the principal (having the relationship with the	14	We agree that the principal who has a relationship with the customer be ultimately responsible for presenting all of the customer-facing requirements of the CDR rules. We also acknowledge that providers

Consumer) to be responsible for ensuring that customer-facing aspects of the CDR regime are delivered (for example, dashboards and any customer-facing communications, including in relation to dispute resolution). We welcome views on this position.		should be disclosed to consumers along with links to the privacy policy, explanation of data use, contact details & complaints process.
Should consumers be able to consent to the disclosure of their CDR data at the same time they give a consent to collect and a consent to use their CDR data? a. Is the proposed threshold for being able to offer an alternative good or service in rule 7.5(3)(a)(iv) appropriate? b. The transfer of CDR data between accredited persons will be commonly facilitated through commercial arrangements. Should those commercial arrangements be made transparent to the Consumer and, if so, to what extent?	15	Part b – Disclosure that the ADR's have entered into a commercial should be disclosed to the Consumer.
To which professional classes do you consider consumers should be able to consent to ADRs disclosing their CDR Data? How should these classes be described in the rules? Please have regard to the likely benefits to consumers and the profession's regulatory regime in your response.	16	We agree with the following list (a) accountants; (b) lawyers; (c) tax agents; (d) BAS agents; (e) financial advisors; (f) financial counsellors; (g) mortgage brokers;

		We do believe registered or qualified auditors should be added to the list. While similar to an accountant, auditors are an independent party who seek to validate a bank account. Their primary purpose would be to validate existence, ownership and value. As auditors are independent, they require their own access to data, separate from bookkeepers, accountants etc.
Should disclosures of CDR data to trusted advisors by ADRs be limited to situations where the ADR is providing a good or service directly to the Consumer? If not, should measures be in place to prevent ADRs from operating as mere conduits for CDR data to other (non-accredited) data service providers?	17	We do agree that a trusted advisor should only be accessing data via an ADR which has a consumer-facing service. This ensures consumers have proper consent management and documented purposes for data collection. We would expect that the trusted advisor's purpose for accessing data be somehow associated with the ADR's purpose for data collection. Should a trusted advisor wish to gain direct access to consumer data they have the right and opportunity to become an ADR We seek clarification for any evidence an ADR should seek to confirm the validity of a trusted advisor. We believe rules should be added to ensure a Trusted Adviser must not share CDR data with another party, being another trusted Adviser, another ADR or a non-accredited party.
Splitting of Consent into 3 distinct consents (Collect, Use and Disclosure)		In the case of a CAP arrangement, does the Provider: • need to store all consents (including Disclosure – of which it may not have a view of) • need to supply all consents (and modifications to said consents) to the data holder so they can present the information on their dashboard – if so, how to notify the Data Holder. • have to provide an endpoint for their Principle to support Disclosure consents maintenance