Australian Banking Association

29 October 2020

ACCC CDR Branch
Via email: ACCC-CDR@accc.gov.au

Dear Jodi,

ACCC Consultation on proposed changes to the CDR Rules

Thank you for the opportunity to comment on the proposed expansions to the Consumer Data Right Rules 2020 (draft Rules).

The Australian Banking Association (ABA) has several concerns with the proposed changes which are detailed in the attachment to this letter. The proposals are deeply complex and the ABA's ability to respond in detail is limited by the consultation timeframe. Equally, ABA members are just days away from the November launch of new CDR functionality, a successful go live must remain the focus of member banks.

The draft Rules intend to allow for the entry of a greater numbers of businesses to participate in the Consumer Data Right (**CDR**) through multiple restricted and unrestricted accreditation pathways. The ABA supports tiered accreditation of recipients however in the absence of detail, the ABA view is that the draft Rules will compromise the security of customer's banking data. The ABA does not support the proposed segmentation of banking data into high, medium, and low risk.

The speed at which the Australian Competition and Consumer Commission (ACCC) intends to finalise the draft Rules is concerning, especially given risks which have been raised in the Privacy Impact Assessment (**PIA**). The ABA does not believe that it is possible for the ACCC to mitigate the risks raised in the PIA and concurrently resolve the questions and concerns raised in this submission by December 2020.The ABA is particularly concerned with negative impacts the speed of implementation will have on smaller banks.

The ABA is also concerned that consumers may be overwhelmed with the level of complexity in the proposed Rules which may make them less likely to participate in the CDR. Trust in the security of the CDR is paramount to its success. The proposed changes to consumer consent, the various restricted accreditation models and the unaccredited model introduce a level of security risk and complexity well beyond what consumers would expect the Government to embed in the CDR.

The CDR is a complex implementation project which has been run to meet arbitrary compliance dates. Future compliance dates need to correlate to the effort and complexity of the task and predicated on the completion of both the Standards and the Rules. Dates should be informed by consultation with industry and consider the limited resources of smaller banks. The ABA believes a project management disciplined, iterative design process between industry, Data Standards Body and ACCC is the best path forward and stands ready to support this process.

The ABA urges the ACCC to reconsider the intention to finalise these rules by December 2020 and seeks a meeting with the ACCC to discuss the concerns raised in this submission.

Kind regards,

[redacted]

Emma Penzo
Policy Director

About the ABA

The Australian Banking Association 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.

Australian Banking Association

1. General comments

Consultation period

The ABA notes the efforts of the ACCC to develop the '*CDR rules expansion amendments – consultation paper – 30 September 2020*' and the '*CDR Rules (Exposure Draft for 3rd amendment – 30 September 2020*' (draft Rules) and the '*CDR Roadmap – Proposed Compliance dates for Consumer Data Right – 30 September 2020*'.[1]

The proposed reforms to the CDR are extensive, deeply complex, and much of it previously untested with the entities which are required to build the CDR infrastructure.

Additional to this, the major banks are in the final days in delivering Phase 2 of the CDR infrastructure. The major banks have deployed staff to work significantly extended hours (including staff who have endured a significant pandemic lockdown in Melbourne) to meet the deadlines of Government and the ACCC. The non-major bank Open Banking project teams are similarly stretched as they seek to deliver Product Reference Data application programming interfaces (APIs) and prepare for the testing phases of the Phase 4 delivery due on 1 July 2021.

Many of the elements of the draft Rules require additional focussed consultation. The Rules for business customers, accreditation, Combined Accredited Persons agreements, consent, and joint accounts are examples.

Privacy Impact Assessment

Update 2 of the CDR Privacy Impact Assessment[2] (PIA) raises several serious concerns.

The PIA raises three general risks (see table below) associated with the draft Rules which are not possible to mitigate within the timeframes issued by the ACCC (that is two weeks from the closing date of this consultation).

A further concern is that the PIA was undertaken concurrently with the drafting of the proposed Rules. This process has resulted in an incomplete PIA. Maddocks (as author of the PIA) notes:

> 'This version includes further proposed amendments that we have not had the opportunity to review and consider whether they pose any additional privacy risks.'[3]

The urgency of the ACCC's timeframes for introducing significant, expansive reforms in a way which raises such significant risks, as noted in the PIA, is unclear to the ABA. The ABA requests that the ACCC publish the CDR roadmap with timeframes that it has been tasked to deliver.

It is the ABA's view that the issues raised in the PIA are significant: the ABA questions the appropriateness of the ACCC Rules editing process over the ensuing two week period and therefore the readiness of the Rules to be made as a formal legislated instrument.

Risk 1: Complexity of the proposed amendments.

Maddocks is 'considering recommending that the ACCC:

- *continue to refine the drafting of the CDR Rules;*
- *issue detailed, comprehensive, and clear guidance about the intended application and operation of the CDR Rules, as amended by the proposed changes. We are considering suggesting that different forms of guidance could be developed and specifically tailored to assist: CDR Consumers; applicants for accreditation; Data Holders.'*

The ABA would endorse such a recommendation. Based on the amount of change contained in the draft Rules, the lack of early engagement with the participants prior to the Rules being drafted, and the

[1] https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0/consultation-on-proposed-changes-to-the-cdr-rules
[2] https://www.accc.gov.au/system/files/CDR%20-%20Update%202%20to%20privacy%20impact%20assessment.pdf
[3] PIA paragraph 1.6 page 4

time period to consider the draft Rules, the ABA does not support the ACCC's position that these Rules can be made in December 2020. Further subsequent consultations using updated and more fulsome technical detail should be undertaken.

Risk 2. Lack of clarity around collection, use, holding and disclosure of CDR data.

The PIA notes that a previously raised issue in PIA Update 1 continues to remain unmitigated. The PIA states:

'As we previously raised in relation to PIA Update 1, we have found it difficult to determine from the proposed amendments which entity or entities will be considered to have 'collected' CDR data in the context of a CAP arrangement, and when that entity or those entities will be considered to be 'holding' CDR data'.

The ABA is concerned that issues raised in previous PIAs have not been addressed by the ACCC. The issue of which entity is deemed to be the 'holding' entity is germane to the privacy and data security requirements of the CDR. Security and privacy of Australian consumers should not be compromised or sacrificed in order to meet an arbitrary deadline.

The ABA would endorse the analysis contained in the PIA. Under the proposed Rules, a Data Holder no longer has clear visibility of which customer's details have been compromised in the likely event of a data breach by an Authorised Data Recipient (ADR) and/or other third parties who would have access to a consumer's data under these draft Rules. Data holders would be incapable of supporting the resolution of issues pertaining to customer data breaches where they cannot determine to whom the data has been transferred.

Risk 3. CDR Consumers will not understand the consents they are providing and will experience "information overload".

The PIA has made it clear that there has been insufficient consideration given to consumer consent. Maddocks notes:

'We are considering recommending that the ACCC consider whether it would be appropriate to continue, in consultation with the Data Standards Body, conducting consumer research on what is the best way to present a CDR Consumer with all of the different types of consents, to ensure that CDR Consumers are provided with an adequate amount of information before providing their consent, but balancing this against the risk of "information overload" for the CDR Consumer'.

The ABA would endorse such a recommendation being made.

Premature and accelerated CDR development

The introduction of change of this scope should not be accelerated.[4] The changes contained in the draft Rules are reflective of a bunching of initiatives rather than an evidence-based market development strategy. It is unclear that the suggestions contained in the draft will achieve the desired outcome to accelerate the consumer participation of the CDR. Rather, customer confusion and inevitable privacy and data breaches will ensue.

Lack of adequate consumer protections

The ABA is concerned that consumers will become overwhelmed with the level of complexity the draft Rules introduce. Some of the changes, particularly the proposed consent framework, introduce a level of complexity to consumers well beyond the knowledge ordinary Australian's have of the CDR and Open Banking – consent, must always be informed consent.

[4] Refer to the ABA submission to the *Inquiry into the Future Directions of the Consumer Data Right*, which has been provided to the ACCC.

Deeper consultation

It is concerning that aspects of the draft Rules have been issued for 'concept testing' – for example, the multiple accreditation models. New concepts (e.g. enclave, trusted advisers etc) should not be first presented to CDR participants as drafted Rules. Rules are not an appropriate vehicle for concept testing.

Character of the draft Rules oscillates

In some parts the draft Rules are expressed as concept in other parts heavily prescriptive and in other parts the draft Rules embed (and therefore pre-empt) the Standards solution.

In summary

Combined, these points indicate to the ABA that this consultation is premature, and the draft Rules are not suitable for finalisation in December. The ABA would be especially concerned, given the breadth and complexity of the draft Rules, if the ACCC were to proceed with a recommendation to the Treasurer for the Rules to be made after only two weeks of ACCC consideration of the feedback from participants and without further engagement with participants.

The ABA strongly urges the ACCC to invoke a best practice systems delivery process as articulated in section 2 *Proposed timelines* of this submission and follow a detailed, iterative consultation process with CDR participants for key elements of the draft Rules.

2. Proposed timelines

The proposed changes increase the complexity and risk of meeting the original current phased obligations. The requirements proposed in the draft Rules, are likely to impact all participant banks regardless of how far progressed they are on the path to delivering the CDR. The original delivery sequence was designed to enable the first Open Banking participants to deliver in a phased approach that provided for the largest and least complex customer segments first (e.g. individual account holders) then moving through to the increased complexity of joint accounts, many-to-sign, and nominated representative accounts. This approach was intended to mitigate the risk of attempting to deliver the solutions for a variety of customer account types in a 'big bang' approach.

The original phased approach is still preferred by the ABA as it provides time for the new technical solutions and operational processes to be embedded across the industry before extending the scope to cover increasingly complex account types and customer segments.

It is important that from this point of the CDR journey that participants, are supported by Government by having a clearly defined set of requirements with adequate time to plan, build, test and launch the solution and supporting operational processes for our customers and colleagues. Increases in scope, such as those proposed in draft Rules, should not impact those phases which are already scheduled. For example, implementation of consent requirements should hold off until data holders have had a chance to implement the original requirements (individual accounts) at the original deadline. The ABA strongly encourages the ACCC to avoid a repetition of the Phase 1-4 build process.

A best practice approach is preferred

The ABA agrees that it is important to establish the main data sharing arrangements for the CDR expeditiously. However, compliance dates *must* be anchored to fixed and detailed requirements.

The ABA notes that where timeframes are set arbitrarily and without reference to the complexity of the underlying requirements, due project management process cannot be undertaken effectively.[5] This is because a systems development requires a stepped process as follows:

[5] The ABA considers the incomplete PIA, and Risks which have not been mitigated as current examples of project governance failures when project management discipline is not invoked.

- A ‘business-requirements gather and confirmation’ stage which delivers a high-level understanding and agreement of how a given aspect of the CDR is to function.
- Customer experience (**CX**) testing which tests different permutations for how the user interface and process flows would operate and helps identify issues upfront.
- Rules development which is iterative and enables sufficient time for deep consultation.
- Standards development (i.e. PRD, CRD, NFR, Register).

It is not possible to determine build times without the final Standards as the Rules do not apply in isolation. The ABA strongly recommends that compliance dates could be recommended by the DSB once build scale has been assessed and quantified in consultation with CDR participants who have assessed the final proposed draft of the Standards. Should the Standards change, then the changes to the target compliance date should follow through invoking a formal change request process.

The forward workplan

The document ‘Proposed compliance dates for Consumer Data Right’[6] proposes compliance dates for functional deliveries for which Standards have yet to be developed. The ABA is strongly opposed to such an approach. It is not possible for the ACCC to determine, and it is not possible for CDR participants to commit to, start dates without the final Standards and Rules and the CX[7]. It is the CX guidelines that support the useability of the CDR, which is critical for consumer uptake.

In determining an appropriate implementation date for the draft Rules, the delivery timeline which has already been locked in needs to be considered. This includes: Phase 3 Feb 2021, Phase 4 July 2021 (over 100 ADIs plus major banks), Phase 5 November 2021, Phase 6 February 2022. The builds for these milestones have been scoped, costed, budgeted, and staff allocations have been set. There is no room for change[8] to the build scope of these deliveries.

The ABA does not accept the premise that some changes do not impact the banks directly, there is very little in the scope of the draft Rules which does not impact banks. Even where scope does not entail bank build, as data holders, banks are required to allocate time and resources to give consideration to those proposed changes in order to confirm the potential level of impact and also to inform the teams of the changes so they remain up-to-date with the CDR.

Provided the Rules, Standards and CX guidelines have been finalised, each element of the draft Rules should be considered for size and complexity of build before a compliance date is determined. The draft Rules delivery should be compartmentalised and implemented with staggered compliance dates commencing no earlier than July 2022 (for initial data holders). The ABA recommends these dates noting that stable and final Standards, and Guidelines would need to be made available and remain fixed for the duration of the scope, build, and test processes leading to the compliance date. During phase 1, 2, and 3 builds, the initial data holders requested a minimum 6-month period between Standards finalisation and compliance date. Some of the builds contemplated in the draft Rules (such as business accounts) are expected to require much more time than the phase 1, 2, and 3 builds.

To illustrate with an example where business account obligation date is set to July 2022: Rules, Standards and CX *must* be in final form no later than September 2021 (and preferably July 2021). This provides from 1 November-July 2021 for the consultation process to be undertaken and finalised.

Timeframes for non initial data holders

Non-major banks are progressing towards their July 2021 entry into the CDR, followed by November 2021 and February 2022 deliveries as required by the existing rules.

---

[6] https://www.accc.gov.au/system/files/CDR%20Roadmap%20-%20Proposed%20compliance%20dates%20for%20Consumer%20Data%20Right%20-%2030%20September%202020.pdf

[7] i.e. PRD, CRD, NFR, Register, CX standards and guidelines.

[8] Other than for emergency fixes.

It is necessary to ensure that smaller banks and FinTechs have certainty and clarity so that they can focus their limited resources on competitive participation in the regime most efficiently. ACCC consideration needs to be given to the significant regulatory impact that the CDR build is having on the smaller banks, particularity a time when banks needed to devote much of their time and attention to maintaining their operations and helping the Australian community during the pandemic period.

The smaller banks have indicated to the ABA that additional scope cannot be added the current scheduled deliveries. The smaller banks do not have the resources to recruit additional staff onto their Open Banking projects nor to outsource development of elements of Open Banking to external consultants.[9] The smaller banks run on tight operating budgets. Their 2021 operating budgets are in the process of being, or have been, allocated. The non-major banks will not be able to accommodate budget-impacting human-resource-impacting new-functionality the following financial year.

Noting that the non-major banks are due to implement the phase 3 products in February 2022, new scope for the non-major banks should not be mandated until after February 2023; although optionality can be provided for non-major banks which may be able to accelerate their deliveries of Open Banking.

3. New restricted models

3.1 A framework for expanding the CDR

The pursuit of CDR expansion should be managed to ensure that data security and customer privacy remains paramount. Expansion without adequate data and consumer protections will limit and negate the effectiveness of existing data security and privacy measures imposed by Australian Prudential Regulation Authority (**APRA**), the prudential regulator of banks. For example, APRA's CPS 234 Information Security aims to ensure that banks take measures to be resilient against information security incidents (including cyberattacks). The CDR should support the requirements of banks. The ABA holds the following principles for banking information security and privacy in the CDR:

Principle 1: All consumer banking data in the CDR adhere to APRA's standards for information security.

APRA's CPS 234 Information Security (and other prudential standards) are the security standards that must apply to Open Banking in the CDR. It is understandable that future sectors may have lower security standards and it may not be practical for CDR participants in those future sectors to uphold the levels of security required in banking. However, it should not be the case that the ACCC mandates lower levels of security for banking data to accommodate future sectors.

The ABA highlights a speech made by APRA member Geoff Summerhayes on cyber security.[10] Mr Summerhayes states: '*there is no room for complacency as cyber-adversaries, regrettably sometimes backed by governments, grow in number and sophistication'*. Further, he states: '*APRA's role in this process is to ensure regulated institutions are resilient to cyber-attacks through prevention, detection and response capabilities.*' Finally, Mr Summerhayes said: '*We've warned repeatedly that it's only a matter of time until an Australian bank….. suffers a significant breach that, in a worst-case scenario, could force it out of business.*'[11]

Principle 2: All consumer banking data must remain within the CDR, there are no sub-sets of less risky consumer banking data.

When banking data leaves the CDR (the security standards which have been designed to adhere to the APRA standards), a security gap is created from which banking data can be accessed and potentially undermine consumer confidence in the CDR and the banking system. A banking data breach by a data recipient whilst causing operational issues for the Accredited Data Recipient (**ADR**), will have far more reaching impacts for trust in the CDR and confidence in the banking system.

[9] Noting that the pool of Open Banking specialist vendors is presently limited.
[10] https://www.apra.gov.au/news-and-publications/apra-member-geoff-summerhayes-speech-to-cybsa-2019-cyber-breach-simulation
[11] https://www.apra.gov.au/news-and-publications/apra-member-geoff-summerhayes-speech-to-cybsa-2019-cyber-breach-simulation

Principle 3: Restricted accreditation for consumer banking data should only be permitted if the entity can partner with an unrestricted ADR

The ABA notes the concerns of small FinTechs which lack the resources to achieve the security standards required for banking data. However, the ABA does not support restricted accreditation whereby that accreditation permits lesser forms of information security and data privacy for banking consumers. The ABA encourages the ACCC to develop models where FinTechs can become a part of Open Banking without compromising banking security standards and consumer privacy standards. The ABA is supportive of a model where a restricted data recipient in partnership with an unrestricted data recipient can execute use cases using banking data provided that the data remains within the CDR and there is no diminution in data security or consumer protections.

3.2 ACCC's proposed models for restricted accreditation

This section deals with the three models for restricted accreditation as proposed by the ACCC.

The draft Rules is not the place to test concepts

In the presentation made to CDR participants at the Data Standards Body call on 23 October 2020, the ACCC noted that it was not necessarily seeking to move forward with all of the models and was seeking feedback as to the feasibility of the models presented.

The ABA submits that a Rules consultation would be more appropriate for testing that the drafting is faithful to the concept or business model it is meant to be representing, as opposed to testing the concept or business model itself. For this reason, this section will deal in concept as per the Consultation paper and not the drafting. The ABA reiterates the need for the ACCC to continue to consult on the most appropriate model(s) of restricted accreditation before it redrafts Rules.

3.2.1 Limited data restriction model

Consumer banking data subsets

The ACCC has sought the views of stakeholders regarding its categorisation of banking data sub-sets into high, medium, and low risk data.[12] The ABA's view is that a consumer's financial and banking data is highly sensitive data and cannot be apportioned into lesser grades of sensitivity. This view that banking data is held to be highly sensitive by the Australian public has been evidenced elsewhere.[13]

Delineating data as high, medium, low risk as proposed in Table 1 raises several concerns:

- The ACCC has not provided its criteria for determining the riskiness of data. The delineation of the sub-sets of the data is subjective and arbitrary. For example, customer data and payee data may be considered sensitive.
- Whilst transaction data has been excluded, bank regular payments are a form of transaction data.
- The data sets suggested by the ACCC are not necessarily distinguishable from those derived from individual transactions.
- Some of the data sets assessed by the ACCC contain personal information.

The ABA notes that 'Insights' of themselves can be as sensitive (if not more sensitive) than the data itself.[14]

[12] Per Table 1 on page 12 of the Consultation paper
[13] 10 OAIC, 'Australian Community Attitudes to Privacy Survey', 2017 https://www.oaic.gov.au/assets/engage-with-us/research/acaps-2017/acaps-2017-report.pdf
[14] This issue is elaborated further in the discussion relating to Trusted Advisers

The risk rating methodology underpinning Table 1 has not been provided in the Consultation paper. Whilst the ABA is not recommending this approach, a framework for assessing data as 'High' 'Medium' or 'Low' risk would be more appropriate for the Rules document rather than the specification of the actual data as Table 1 currently does.

Future sector data washing

This model does not anticipate the risk to consumer privacy and security from future-sector data washing potential. For example, a combination of the data contained in the data sets 'Basic Bank Account Data' and 'Basic Customer Data' (per Table 1) can yield deep customer insights. When combined with Energy data sets the potential for insights which even the consumer would be unaware of would be manifold.

How a restricted accreditation may work

The ABA does not support the Limited Data Restriction model on the basis that all banking consumer data is highly sensitive (consumer privacy) and high risk (financial stability). Where entities are unable to meet the security and privacy requirements for consumer banking data, they may choose to partner with unrestricted ADRs to participate in the CDR in a manner that ensures no diminution on the security of the data or existing consumer protections.

3.2.2 Affiliate restriction

The Affiliate restriction is a high-risk model for expanding participation in the CDR (for Open Banking):

Data daisy chain

This model enables the creation of a 'daisy chain' of data being passed from one ADR to another which will put the onus on the consumer to know where their data has been sent, for what purpose and duration. The consumer will be required to manage multiple ADR sites to maintain and adjust consents. It is unclear how the consumer will know where the responsibility for their data lies. The data holder will have no visibility and therefore unable to support the consumer in the event of an issue or a breach.

Profit motive

The affiliate model enables the sponsoring ADR to charge for data which it has freely accessed from the data holder. The monies charged will inevitably be paid for by the consumer.

Divestiture of accreditation responsibilities

Under this model, the sponsor can determine if another entity meets the standards of accreditation. The ACCC has divested its responsibility as an accrediting and oversight body of Accredited Data Recipients. The ACCCs controls appear inadequate relative to the risk that this model introduces.

The ABA does not support the affiliate restriction.

3.2.3 Data enclave restriction

The ABA understands that the Data enclave restriction will operate within the structure of a combined accredited person (**CAP**) arrangement. The enclave model at this conceptual level adheres to the principles noted by the ABA:

- Consumer banking data will be secure because an unrestricted accredited data recipient will provide the security structures.
- All consumer banking data will remain within the CDR as the principal will have access to the data through the sponsor, without having the ability to transmit the data externally.
- The restricted ADR is in partnership with the unrestricted ADR to execute on its use cases.

The data enclave model could potentially increase participation in the CDR whilst protecting consumer banking data. The ABA notes the ACCC's Questions 8 and 9 in respect to data enclaves and suggests that the ACCC develop this concept further to reconsult with participants. As the model solidifies the ACCC should undertake CX testing after which the Rules should be redrafted.

4. Combined Accredited Person arrangements

The CAP arrangement model could be the mechanism by which entities which cannot be accredited as unrestricted ADRs enter the regime. The CAP arrangement model should be afforded time to be tested and to mature in operation.

To ensure the robustness of the CAP arrangement model, the ABA recommends the ACCC provide further clarification in the draft Rules in respect to its operation and the responsibilities of the parties within the CAP arrangement.

Specifically, the ABA refers to the recommendations contemplated by Maddocks in the PIA.

Risk	Maddocks analysis/ recommendation	ABA position
'The CDR Rules do not deal with a situation where the relevant CAP agreement is terminated, or suspended, or expires'.[15]	Maddocks is 'considering whether there should be a requirement in the CDR Rules (or perhaps a condition of accreditation) to notify the Data Recipient Accreditor if the relevant CAP arrangement is suspended or terminated or expires, and for the Data Recipient Accreditor to have the ability to suspend or revoke the restricted accreditation in such a situation.'[16]	Support
'A provider under a CAP arrangement may not comply with a direction by the principal to delete redundant data'.[17]	'It is not clear whether Rule 7.12(2)(b) will apply to a CAP arrangement for data enclave accreditation arrangements… [T]here does not appear to be any legislative requirements for the provider to comply with a direction by the principle in respect of redundant data.'[18] 'We are considering recommending that this be further clarified by the CDR Rules.'[19]	Support
'[O]nly the principal… will be required to keep records about the CAP arrangement'.[20]	'We are considering that the ACCC consider whether there would be benefits in broadening Rule 9.3(2)(i) to apply to providers in a CAP arrangement.'[21]	Support

The ABA supports the disclosure of the nature of the CAP arrangement to consumers on the basis that it is the totality of the entities of the CAP arrangement which are delivering the proposed benefit to the consumer. The CAP arrangement disclosure should specify the roles and responsibilities of each entity in the CAP and the process for complaints management. Such a disclosure is no different to that which is made under white label arrangements for banking products – where both brand and ADI are disclosed.

[15] PIA Issue #29 p74
[16] PIA Issue #29 p74
[17] PIA Issue #31 p76
[18] PIA Issue #31 p76
[19] PIA Issue #31 p77
[20] PIA Issue #33 p78
[21] PIA issue #33 p78

Australian Banking Association

5. Unaccredited Trusted Advisors

The ABA is strongly opposed to the diminution of the CDR security and privacy standards as proposed by the Trusted Advisor model (**TA**). All the preceding ABA comments in respect to newness of the concepts in the draft Rules and lack of detail and consultation applies to the TA model proposal.

The ABA considers that the TA model significantly deviates from the Open Banking Report by Scott Farrell.[22]

The Open Banking Report clearly envisaged a regime where data recipients of banking data would be accredited at various levels[23]:

> *'Recommendation 2.7: **Only accredited parties** should be able to receive Open Banking data. The ACCC should determine the criteria for, and method of, accreditation'.*
>
> *'Recommendation 3.10: Authorised Deposit-taking Institutions (ADIs) should be automatically accredited to receive data under Open Banking. A graduated, risk-based accreditation standard should be used for non-ADIs'.*
>
> *'Recommendation 4.8: 'In order to be accredited to participate in Open Banking, **all parties must comply with designated security standards set by the Data Standards Body'**.*

The Open Banking Report clearly acknowledged the significantly higher standards of security required by APRA than was then required through the *Privacy Act*:

> *In respect to the security standards applicable in the banking sector, the Open Banking Report said: APRA's requirements effectively set security standards for customer banking data that go beyond the requirements of the Privacy Act.'*[24]

The Open Banking Report was clear in the importance of an accreditation process to foster customer trust:

> *'From the customer's perspective, an accreditation process is desirable. Accreditation would allow customers to determine with greater ease which data recipients meet the Standards and may, as a result, be considered trustworthy. An accreditation process should inspire confidence amongst consumers to share their data with recipients that the customer has chosen to trust. An accreditation process would also provide same level of customer protection from malicious third parties.'*[25]

The Open Banking Report acknowledged that there may be a place for a non-accreditation for future sectors but not the banking sector:

> *'The review notes that, in conducting assessments for future CDR sectors, the ACCC and OAIC may conclude that a sector does not require accreditation.'*[26]

The proposed TA model deviates from the principles identified in the Open Banking Report. It allows unaccredited entities to access banking data, which is highly sensitive, into a business environment which is governed only by the *Privacy Act* and which the Open Banking report acknowledged does not support the significant APRA set security requirement of banks.

The ABA does not support the TA model.

[22] https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking-_For-web-1.pdf
[23] Bolding has been added by the ABA
[24] See Open Banking Report page 63
[25] See Open Banking Report page 22
[26] See Open Banking Report page 22

The ACCC queries the disclosure of 'derived data' and 'data insight' disclosure. Insights are gleaned from algorithms or analysis which infers or makes conclusions in respect to a customer trait, tendency, or behaviour.

There are moral issues associated with the disclosure of such data. These are exemplified in the following scenarios:

- The deduced trait (i.e. the insight) may be accurate, but the customer may not be conscious of it. In this case, the passing of data about a customer trait of which the customer may/may not be conscious to a TA should not be permitted on the basis that the data is being disclosed to an unsecure environment and the consumer is unaware of the nature of the trait being disclosed.
- The consumer may disagree with the deduced trait (i.e. the insight) and may challenge the assumptions and analysis by which it was derived. In this case the disclosure of the trait would have been made into an unaccredited environment before the customer had the opportunity to challenge the insight and ask for its deletion.

The ABA suggests that an insight should be de-identified, aggregated data which does not relate to individual consumer records (for example average loan amounts derived from a number of consumer accounts).

The ABA recommends that insights as defined not be permitted to be disclosed outside of the CDR.

6. Business & Commercial Customers

6.1 Business channels

Build time

There is significant complexity in the CDR build for business accounts which is attributed to the enablement of the authorisation process. The variety of legal structures, legal documents, authority levels, and signatories to the account requires careful analysis. An initial delivery that includes all business products that are already available through a bank's primary business online channel is feasible. Extending this to other products should be considered as a subsequent phase.

The ABA's view is that timelines should be set as outlined in Section 2 of this submission.[27] If this is not possible, at least 12 months should be allowed from when the Rules and Standards are final. The runway to the compliance date must be clear of other deliveries. If business accounts are to be the next major delivery of Open Banking, based on existing compliance dates, the ABA suggests such a delivery should not be contemplated before July 2022 for initial data holders and July 2023 for non-initial data holders[28].

Migration limitations

The position of the ACCC is that where business customers are housed in complex business channels, they are to be also accommodated in the main business channel if that customer opts to utilise the CDR.[29] This is helpful because some banks offer more than one business banking channel. However, banks will be limited in the extent to which such migration can be achieved.

Complex business customers may be supported by their bank via a variety of business banking channels.[30] Typically, these customers require greater functionality. Additionally, complex, bespoke products outside the scope of CDR may be held in backend IT systems and only integrated with the complex business banking channels. Therefore, customer migration to the primary business channel could be blocked because the primary business banking channel will not be able to provide a full picture of a customer's arrangements. This will result in a sub-optimal business banking experience for these

[27] See section 'A best practice approach is preferred'
[28] Provided no additional obligation dates with associated builds are imposed beyond that which is currently scheduled
[29] Consultation Paper p24
[30] That is, not the primary business banking channel.

banking customers. The ABA questions the benefit attainable by sophisticated corporate customers through the CDR. Sophisticated corporate customers will typically have in place arrangements to access their data directly via their banking provider and will be unlikely to go through an ADR for that data.

The ABA recommends that the ACCC adopt a flexible approach in respect the relevance of the CDR to sophisticated corporate banking customers.

Nomination process

The process by which nominations are made requires further thought. Examples of questions requiring resolution at the Rules or Standards level include:

- Who can nominate users to access a corporate account?
- Can individuals nominate themselves?
- What evidence is required by the Data Holder – e.g. board/director approval?

The ABA recommends that the ACCC consult further on the nomination process and consider whether this is best left to the data holder to address outside of the Rules and Standards.

6.2 Specific rules for business partnerships

The ABA does not believe that specific rules are required for business partnerships. As per the advice provided by the ACCC, banks' Phase 1, 2 and 3 implementations will accommodate partnerships where those partners are joint account holders.

More complex business partnerships with nominated accounts will be treated as per other businesses through the primary business channel.

The ABA supports flexibility in implementation and does not support rework which will see the implementations done (or planned) for simple partnerships in the retail channel as per advice from the ACCC to be undone.

6.3 Secondary users

General feedback

The business case for the inclusion of secondary account users has not been established. Further consultation is required to clarify or define issues such as:

- The intended differences between a Nominated Representative and a Secondary User. Is a 'nominated representative' intended for non-individuals/companies, whereas 'secondary user' is the terminology intended for individual customers? A requirement gathering and consultation phase would help a shared understanding of examples where they would/could be used.
- How does a Power of Attorney (**POA**) fit with this construct? Is the POA a nominated representative or a secondary user?
- Account privileges, as there are existing relationships for Secondary Users (POA, Enduring POA, Third Party Signatories, Trustees)?
- For secondary users on joint accounts does one or both joint account owner(s) nominate?

The ABA suggests that the intersection between joint accounts and secondary users is potentially complex from a Rules (and thus an implementation) perspective. The ACCC might consider a simpler approach in the short term (such as restricting such a function to sole accounts only) until there has been further consideration and consumer engagement on the matter.

Further, the ABA strongly suggests that secondary users must have an existing account relationship (e.g. third party signatory, POA, etc.) before they can be allocated secondary user status in the CDR; the alternative (where the secondary user has no existing relationship to the account) is far more complex from an implementation perspective and will likely conflict with established account keeping governance rules.

The ABA recommends that the draft Rules relating to Secondary Users require further consideration and consultation with participants to identify the underlying objectives for secondary users in the CDR.

Detailed feedback

Section of the Proposed Rules	Feedback
Rule 1.13 (e) (i)	Does the 'service' need to be online?
Rule 1.15(5) Consumer dashboard - data holder	• Concerns around the amount of detail required to be available on the Consumer Dashboard without any specific CX Guidelines. • Will CX guidelines be issued for how data holders are expected to amalgamate this service into the consumer dashboard and/or JAMS service? • How will the nomination of secondary user work for joint accounts? Do all joint account owners need to agree on the nomination of a secondary user? • If consent set up by owner and secondary users for same account with same ADR is that an issue?
Schedule 3 Clause 2.1(1) Meaning of eligible - banking sector	Are data holders required to check the account owner's eligibility **AND** the eligibility of any secondary user? • If yes, is the expectation to check all of the customer eligibility during grant consent flow and banking API call (i.e. during data-sharing)? • If yes, are the eligibility checks the same for the owner(s) and the secondary users and nominated representatives? • If yes, what happens to an existing consent where the secondary user/nominated representative access has been revoked? The requirement for a pre-approval option to be in place for a joint account when nominating a secondary user: is the intent to ensure that at least one joint owner is across and approves any consent granted by a secondary user?
Schedule 3 Clause 4.8(1) Consumer data requests that relate to joint accounts	• Does a secondary user automatically see any existing consents for an account on their dashboard once they have been nominated as a secondary user? • Can any secondary user see what is set up by other secondary users if they have access to the same account? • Can a secondary user revoke a consent set up by the owner or other secondary users?

Australian Banking Association

7. Joint Accounts

In-line elections

The standards as the appropriate instrument

The ABA questions whether it is appropriate for Rules to prescribe the process flow for account election. Such prescription in the Rules is not aligned to a principle-based approach for the Rules.

More CX is required

It is important for CX to be reflected in the Standards for how joint accounts are to be elected as participating accounts in Open Banking. However, the ABA notes that there have been significant and detailed questions raised about the quality of the customer experience in the event where an account is not available for a customer to approve or select in an in-line election. It is possible that an in-line election function may result in no data being shared. This indicates that further CX is warranted and these Rules and Standards are not ready for finalisation.

November 1 build is disposable code

The draft Rules is prescribing rework on in-line joint account election builds that have yet to come into production. Joint accounts are due to be made available by the initial data holders on 1 November 2020 in accordance with the ACCC mandated timelines. Newly minted code cannot be treated as disposable and banks required to re-develop their solutions. This disadvantages participants who have invested significant resources to meeting an accelerated timeline of 1 November and also jeopardises the code deliveries of non-initial data holders, who have scoped their builds for 2021 according to the current Rules. This rework is the consequence of a process which has been led by an arbitrarily set deadline (1 November) and not one which has followed best practice project management delivery.

The ABA suggests

The Standards, as opposed to the Rules, should provide more optionality in respect to how these joint account elections should function. The Standards should support multiple flows and allow as much decision making as possible to the competitive space.

Other feedback

The ABA has identified the following additional issues:

(a) Number of Joint account holders:

In practice, it is possible for an unlimited number of Joint Account Holders to be associated with an account. In practice, most joint accounts are associated with at most two persons. A requirement to cater for any more than two account holders will significantly complicate the CX and usability of the joint account service.

The ABA recommends that Joint Accounts should be limited to two account holders.

(b) Draft Rules requiring clarification

Section of the Proposed Rules	Feedback
4.4 Simplified outline of this Division	Clarification is required on the details in the clause that starts with: *Neither disclosure option applies to a joint account if...* Does this mean that DH do not need to enforce an option being selected? **OR**

	Do the owners have to positively elect they do not want to apply a disclosure option (preference)?
	• If they need to positively elect, then do data holders need to provide three options as follows:
	  o Pre-approval (MUST provide)
	  o Co-approval (Optional to provide)
	  o No preference required (MUST provide??)

4.5 Disclosure options that can apply to joint account	• What is expected to happen to any existing consents on joint accounts that are active at the time this rule comes into play, as they will not have a disclosure option nominated by owners? • Is this covered in the above point about where the owners have not indicated a disclosure option? (See scenarios below)
4.6 Obligation to provide joint account management service (JAMS)	• Clarification on how data holders are meant to handle the situation where a different disclosure option is selected by joint owners. i.e. do the data holder not enable the account for data sharing until this the disclosure aligns? • Are there any CX guidelines that cover this or to cover JAMS in general? • Concerns around the amount of information data holders need to disclose as part of (7) given that a consumer may be selecting a disclosure option as part of a consent (authorisation) and this will not be simple and easy to provide.
4.7 Asking other joint account holder to indicate disclosure option for joint account	• Does this need to occur as part of JAMS? (See scenarios below for questions relating to this clause) (e) covers if they agree to same option. However, it does not cover the scenario where they do not want the same option. What needs to happen then? • 4.7 (2) this section has been interpreted to mean that the data holder is responsible for contacting other joint account holder/s every time an election is made or changed and explaining their options. The ABA does not support this requirement
Rule 4.10	The requirements of this clause are unclear. The ABA suggests that the ACCC should clarify the term 'disclosure option'
4.11 Asking account holder B for approval to disclose account data	See scenarios below for questions relating to this clause.
Schedule 3 - 1.2 Interpretation **Joint account definition**	Some ABA members have joint accounts owned by more than 2 individuals and in some cases they have **more than four owners (>4)**. It is unduly complex both from customer experience perspective and technically to cater **for >4 owners.** The ABA suggests that a limit to the number of joint owners be imposed as there are diminishing benefits of catering to low volumes.

(c) Joint Account Scenarios requiring clarification

Scenario 1: Joint account with an existing election but no preference nominated (In Flow)

Customer A has set up a consent with ADR1 that contains a joint account owned by Customer B and this consent has been in place since December 2020.

- Once these rules changes take effect, the customers determine they would like to set up a consent with another ADR (ADR2).
- Customer A commences the grant consent (authorisation) and selects a joint account that is owned with Customer B.
- There is currently no disclosure option (preference) set for this joint account.
- As part of this consent flow (authorisation) once accounts are selected on the data holder side the data holder detects there is no preference for this joint account and therefore the data holder provides the option for customer A to select a preference for this account.
- Customer A selects a pre-approval disclosure option for the account.
- A notification is sent to Customer B advising them that Customer A has nominated a preference and requires them to approve/reject.

What is meant to happen next?

- Customer A would be navigated back to the ADR. However, until Customer B selects the same preference, is the data holder allowed to data share on this joint account?
- What happens to the existing consent that has been in place since December 2020? Does the data holder need to stop sharing on the joint account until Customer B selects a preference?
- If the new consent contained accounts solely owned by Customer A along with the joint account owned with Customer B, can the data holder share data for the solely owned accounts OR does the data holder need to wait until it gets a preference option from Customer B on the joint account?
- How do data holders represent this activity to both customers from a CX perspective? What are the rules and guidelines for this?

Further, there appears to be a new 'pending' state anticipated in the draft Rules:

As described in this scenario, customer B needs to act on the authorisation request from customer A.

With reference to the accompanying CX expansion pack wireframes[31]: This shows the ability for a joint account to be selected as part of an authorisation even when elections are not yet in place. It then has this account as 'pending' until the other joint account holder elects.

It's notable that a new state – **pending** – is envisioned as part of the in-line election flow and that this potentially creates complexity and ambiguity in terms of the state of the account sharing as well as the overarching authorisation (and any other accounts therein). Managing a 'pending' state of sharing will have both technical and CX implications.

The ABA requests further detail on the proposed Rules and implementation approach to manage this state.

[31]Refer to 7.1 Sharing CDR data on joint accounts: https://consumerdatastandards.gov.au/wp-content/uploads/2020/10/CDR-Rules-Exposure-Draft-CX-Wireframes.pdf

Scenario 2: Joint account with an existing election but no preference nominated (JAMS)

Customer A has set up a consent with ADR1 that contains a joint account owned by Customer B and this consent has been in place since December 2020.

- Once these rules changes take effect, the customers determine they would like to set up a consent with another ADR (i.e. ADR2).
- Customer A signs into the Joint Account Management Service (JAMS) and selects a joint account that is owned with Customer B.
- They nominate a disclosure option (preference) for this joint account.
- A notification is sent to Customer B advising them that Customer A has nominated a preference and requires them to approve/reject.
- Customer B signs into the Joint Account Management Service (JAMS) and selects the joint account that is owned with Customer A.
- They review the preference nominated by Customer A and they nominate the same preference (or approve the preference set by Customer A).
- A notification is sent to Customer A advising that the preference is now set for this account.

What is meant to happen next (pre-approval set)?

a. Customer A grants consent (authorisation) to another ADR based on the pre-approval disclosure option selected. As pre-approval option is nominated, no further approval required by Customer B.

   Where co-approval option was nominated, must ALL other account holders approve the consent (authorisation) prior to it be executed?

b. Once the consent (authorisation) is granted, Customer B is notified and can see the details on their Consumer Dashboard

   Where co-approval option was nominated then ALL other account holders are advised of outstanding consent and when they all approve, they can see the consent (authorisation) on their Consumer Dashboard.

Is this understanding correct?

(d) Joint account definition

In Division 3.1, the definition of a joint account remains unchanged - "For the banking sector, special rules apply to joint accounts with two (2) individual joint account holders" - with the addition of accounts with more than two (2) account holders, what is the expectation with respect to these? Why would rules applying to accounts owned by two (2) not apply to accounts owned by three (3) or more?

(e) On-disclosures to joint account holders

The ABA does not support this requirement as it is potentially technically complex with limited value. Any on-sharing arrangement and the authorisation of such an arrangement should be managed by the ADR.

Australian Banking Association

8. Consents

The proposed consent framework introduces a level of complexity to consumers which may not support informed consent being given.

Amending consents

The Rules should be silent on the technical implementation requirements: this is the function of the Standards. Through the iterative design process, the ABA would like to understand the 'simplified' authorisation in more detail as we need to assess any technical impacts as well as any impact on existing risk controls.

Separate consents approach

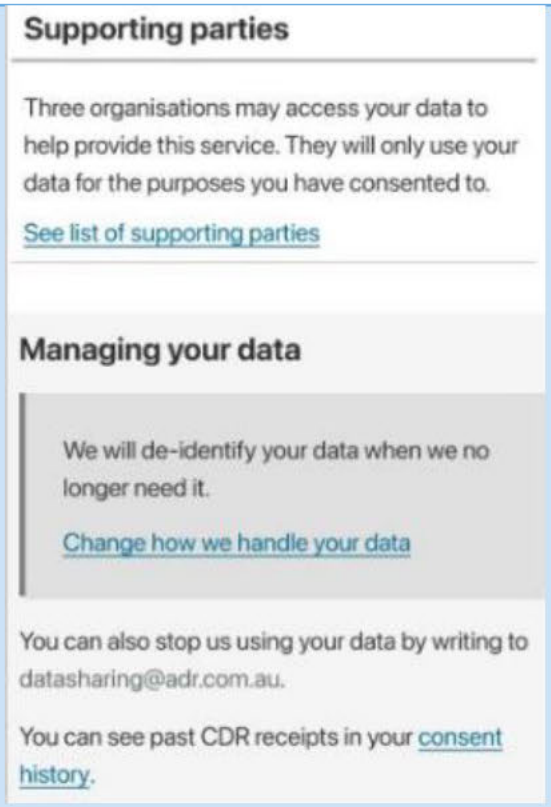
The ABA notes that the ACCC has recently introduced different use and collect consent periods. The draft Rules introduce another new requirement to create different consents. Although this Rule does not impact on data holder builds, the ABA queries the need for this level of consent separation and the priority which has been given to this functionality. The ABA would like to see which use cases these consents are intended to support and the business case for how they will drive additional competition and consumer protection.

Data holder dashboard

The Rules should be silent on the technical implementation requirements: this is the function of the Standards. Participants will provide feedback in GitHub on how the ADR and their software product should be represented in the authorisation and dashboard user experience. The proposed rules would create an implementation burden on data holders particularly if there is flexibility and variability in the way in which ADRs wish to apply the taxonomy in different CX scenarios. A consistent and prescribed approach in which data holders are required to display these attributes, would lessen the implementation burden.

Detailed feedback

Section of the Proposed Rules	Feedback
Rule 1.10A Types of consents	• Clarification on the separation of Collect/Use consent: From a customer's perspective, why would customers consent to 'collection' without 'use'? Could the ACCC provide an example of a COLLECT use-case only? • From the CX wireframe guidelines, it appears that the different consent types are combined, despite the distinction of consent types in the rules. Is the distinction in the rule intended to be a legal construct or are there functional/technical changes that are expected to how consents are managed within the ecosystem?

	 • If all consents need to be related/are in a hierarchy: o What are the dependencies (if any) between consent types? o What is the implication for revokes? For example - If there is a collect, use and disclosure type and a collect is required for a use consent and a disclosure, then if the collect is revoked would this mean that all related use and disclosure consents need to be revoked? • Regarding Trusted advisors and Accredited persons: o Does the data holder have to keep track of the final destination of the data and update the customers dashboard to state this? o Who validates the eligibility of the Trusted advisors? What if the trusted advisor becomes disqualified? Is the data holder expected to validate this eligibility? • Suggestion for multiple types of consents for customers – Ability for customers to name their consents i.e.: Adding a "Nick name"
Subdivision 4.3.2A Amending consents	• Clarification required for joint accounts. Will all joint account holders have to approve all amendments?
Rule 4.12A and Rule 4.12C	• The outlined changes in the rules is conflicting, in 4.12C it requires amending consent to happen in the same way consent was originally authorised. Rule 4.12A mentions the use of the consumer dashboard.
Rule 4.18A Notification if collection consent expires	• Customers may have multiple consents with ADRs and may lose track of these. Dependant on the type of expiry, does the data holder need to inform the customer that their data has been deleted at a point in time?

9. Other

9.1 Over-compliance

The ABA requests guidance from the ACCC in respect to how it will address over-compliance. How can a data holder place reliance on 'good faith' provisions under 56GC of the Act if the Rules note that what is not required, is not permitted/authorised?

> **56GC Complying with requirements to provide CDR data: protection from liability (1) If: (a) a CDR participant, or designated gateway, for CDR data (the CDR entity): (i) provides the CDR data to another person; or (ii) otherwise allows another person access to the CDR 1 data; and (b) the CDR entity does so, in good faith, in compliance with: (i) this Part; and (ii) regulations made for the purposes of this Part; and (iii) the consumer data rules; the CDR entity is not liable to an action or other proceeding, whether civil or criminal, for or in relation to the matter in paragraph (a).

Currently the note on Rule 1.13 states that such disclosure is neither required nor authorised, and this is a general theme in the Rules, that what is not required (or specifically optional) is not authorised. This differs from other protective regimes such as the NCCP, e-Payments code, Unfair Contract Terms, Banking Code of Practice etc., where following the regime, which is protective in being a secure mechanism, is permitted even if the consumer is not eligible. For a regime which is both protective from the risks of screen-scraping, and enabling greater control for consumers, this attempt to draw a bright line between compliant and required vs not required therefore non-compliant is problematic and also causes operational complexity.

9.2 Miscellaneous

Section from the Expansion amendments consultation paper	Feedback
Section 8.1 Product reference data rules for white-labelled products	• Although not necessarily aligned with previous guidance, the ACCC may wish to consider an approach where the party that manages (a majority) of the product reference data, such as rates and fees, might be best placed to meet any disclosure obligations. It is possible that a white-labeller may hold contracts with consumer, but not set rates and fees, for example. • The possibility of multiple data holders meeting a product reference data obligation simultaneously as allowed but not required in 2.3 (4) should be avoided. The current data standards for product reference data have significant flexibility in the representation of products, and duplicated, distinct representations of some products would create difficulties for data recipients. For example it would be desirable to avoid a situation where there is a single credit card product with similar representations from multiple data holders because it would be technically difficult for data recipients to avoid duplication in their use cases. • The register is not currently designed to support the technical discovery of product reference data. The current entity model does not have a way to represent one legal entity sharing product

	reference data on behalf of another. For example, a grocery retailer could only be represented as a 'brand' of a financial services legal entity at present. Changes to the entity model of the register may have flow on impacts for consumer data request services. • The proposed approach may not generalise well to consumer data requests – the party that enters into contracts with customers may not manage the customer experience components or brand through which customers would grant consent. Thought will need to be given to the evolution of the register so that there is flexibility for different entities to provide different technical components. For example a brand owner might provide components related to authorisation and consent management, whereas a white-labeller might host and share data where authorisation exists. • Flexibility between data holders to meet obligations based on contractual arrangements is welcome.
Section 8.5 Registrar amendments	• Clarification on how these rules would operate in practical terms. E.g. How will the participants be informed or how the "opportunity to be heard" will operate. • Clarification is required on how quickly the block is to be implemented. • Does the data holder need to be heard before it blocks activity?
Section 5.1 Disclosures to Trusted Advisors	• How does a CDR consumer practically nominate a trusted advisor? • What is the relationship between consents? Clearly a collection consent is initially required for other consents to be meaningful. Are there other relationships? How do they evolve over the lifecycles of consents? Are insight disclosure and trusted advisor consents independent? Can one exist without the other? • Introducing the ability to share to trusted advisors introduces increased risks for customers and reputational risk for data holders. How will the status of trusted advisors be validated by ADRs? Is it acceptable for ADRs to limit to a finite list of trusted advisors? • Will the involvement of trusted advisors be shared with data holders? This would require changes to grant and manage consent processes. It may be difficult for customers to manage concurrent authorisations without the ability to see information associated with that information. However, practically allowing this information to be displayed by data holders would require changes to the data standards.
5.2 Disclosures of insights / Use of CDR data for research	• What is the distinction between general research / creation of insights?
Schedule 3, Part 2, 2.1	• 'Meaning of eligible' appears not to address nominated representatives on business accounts. They should be listed here in the same way that secondary users are listed. Based on this definition banks would not have any eligible customers who are businesses.