AUSTRALIAN
RETAIL
CREDIT
ASSOCIATION

The Treasury
Langton Crescent
PARKES ACT 2600
Via email

23 March 2018

Thank you for the opportunity to provide a submission on the *Review into Open Banking in Australia – Final Report* (the Review).

For background, the Australian Retail Credit Association (ARCA) is an industry association with the objective to promote the integrity of the credit reporting system, enabling better lending decisions. In this respect, the 'credit reporting system' includes the system as established under *Part IIIA* of the *Privacy Act* (Part IIIA) and also the broader range of data available to credit providers to assist with credit decisioning.

ARCA's members are drawn from both credit providers and credit reporting bodies. Credit provider members include the thirteen largest APRA regulated banks, and a broad range of fintechs, finance companies, and credit union and mutual credit providers. Collectively, ARCA Members account for over 95 percent of all consumer lending by dollar volume, and over 80 percent by number of accounts. Furthermore, the four national credit reporting bodies are all ARCA Members.

ARCA supports the concept of Open Banking on the basis that the availability of more data in the system, that is available to a broad range of entities for a wider range of purposes, is good for competition and for consumers.

However, in order to ensure that the competition and consumer benefits are fully realised, any data sharing arrangements require careful design:

- To maintain the integrity and reputation of the system
- To ensure participants don't abuse their access to consumer data
- To protect consumers
- To make the system efficient and to operate at a low cost
- To provide certainty to participants around what behaviours are acceptable
- To ensure fairness between participants

In the main body of this submission we set out some higher-level policy observations on the operation of Open Banking. In *Annexure One* we set out some feedback in respect of specific Review recommendations.

POLICY OBSERVATIONS

Timing

We believe that the 12-month implementation timeframe proposed in the Review is ambitious – particularly given the need to ensure that, as discussed below, the regulatory frameworks adequately protect consumers and that industry frameworks are well designed and effective. We also note that, despite banks being aware of the proposed introduction of Open Banking, proper preparations are not possible until the detail of the model is known.

Industry's role in developing the Rules and Standards

There are many similarities between the proposed implementation of Open Banking and the introduction of comprehensive credit reporting (CCR), particularly in terms of the exchange of consumer data between a broad range of industry participants. ARCA played a significant role in facilitating the implementation of comprehensive credit reporting and our experience may provide useful insights into the challenges involved for Open Banking.

For example, the *Privacy (Credit Reporting) Code 2014* (CR Code) – much like the proposed Rules for Open Banking – builds upon the general legislative requirements for credit reporting as detailed under *Part IIIA* of the *Privacy Act*, providing a further level of detail in respect of the operation of the credit reporting system. The Privacy Act allows the Information Commissioner to appoint a 'code developer' to develop the rules under Part IIIA, and ARCA was appointed by the Information Commissioner to be that code developer. Those rules (i.e. the CR Code) were then reviewed and ultimately registered by the OAIC.

Importantly, the instructions for ARCA as code developer required it to develop a "balanced" code that took into account the interests of all stakeholders. This put the industry's knowledge and experience to use to develop the CR Code, and did not detract from the opportunity for all stakeholder groups (across industry sectors and consumer groups) to participate and be consulted during the process. Ultimately, appointing ARCA as code developer did not change the OAIC's role as the ultimate decision-maker in terms of whether the CR Code was appropriate for registration.

Likewise, ARCA played a central role in developing the *Principles of Reciprocity and Data Exchange* (PRDE) and the *Australian Credit Reporting Data Standards* (ARCDS), which, respectively, establish a set of business-to-business rules for credit reporting that encourage a competitive and efficient sector and ensure that the data shared in the system is consistent and meaningful.

Treasury has recently undertaken a process to develop the *National Consumer Credit Protection Amendment (Mandatory Comprehensive Credit Reporting) Bill 2018* (Mandatory Bill) – which will, once passed, require the four major banks to supply their credit information into the Part IIIA credit reporting system. We have also had the opportunity to assist Treasury in building their understanding of the credit reporting system and the challenges involved in mandating the supply of data.

In developing the Rules for Open Banking, the ACCC will likely need to develop not just the 'business-to-consumer' rules (the CR Code equivalent), but also the 'business-to-business'

rules (the PRDE and ACRDS equivalent). Given the complexity, this will be a difficult task for the ACCC to undertake.

In developing the PRDE, ARCA was required to develop detailed business-to-business rules relating to issues such as disputes between businesses, as well as detailed requirements for 'reciprocity', including key principles such as participation levels and exceptions. Such rules are very difficult to replicate in legislation, and to be effective and fair require significant consultation and iteration between industry participants with very different interests and operating models.

For that reason, we recommend that the Open Banking regulatory framework include an ability similar to the Privacy Act to allow the ACCC to appoint a 'Rules developer' (which would be an industry representative) to undertake the initial consultation and drafting of the industry specific Rules, which would then be registered by the ACCC.

We set out some additional matters for consideration, and specific suggestions, in respect of *Recommendations 2.4, 2.11 and 3.9* in *Annexure One*.

Consent and Consumer Protection – and the need for certainty for industry

The Open Banking regulatory regime must strike a balance between consumer protection and innovation. If there is a lack of adequate consumer protection, this will undermine consumer trust in Open Banking. From an industry perspective, a robust consumer protection framework will reduce the risk of things going wrong in the future that could otherwise result in an overly restrictive regulatory response.

The Review proposes a consumer protection framework that seeks to ensure the privacy and security of the consumer's data, including a consent framework that seeks to put the consumer in 'control' of their data. This is to be done by requiring a customer's consent to be 'explicit, fully informed and able to be permitted or constrained accordingly to the customer's instructions' (*Recommendation 4.5*) and requiring a simple, 'single screen' notification of the uses to which the consumer's data can be put (*Recommendation 4.6*).

While it seems reasonable to require a clear and simple consent process, it also seems reasonable to suggest that the objectives of ensuring the consumers are fully informed and requiring the consent process to be streamlined (i.e. 'single screen') are potentially at odds with each other.

The Review also notes the likelihood that consumers will be asked to accept "terms and conditions of service (by clicking on 'I agree' on a screen), without … having any real choice but to agree if they want the service".[1] That is, the product issuer or service provider will make the provision of the product or service conditional on giving consent. Merely requiring those consents to be clearly worded and explicitly acknowledged by the consumer will not automatically mean the consumer remains in control of their data.

In contrast, in relation to credit reporting, Part IIIA of the Privacy Act, which permits the exchange of consumer credit information between credit providers and credit reporting bodies

[1] Review, page 51.

subject to giving the consumer *notice* of the exchange, imposes strict limitations on the circumstances in which that data may be used and disclosed.[2] That is, the use cases for which the information can be put are set out in the law and are not subject to extension through the consent of the consumer.

We do not propose that the Open Banking regime impose any such strict limitations. Given the nascent state of the Open Banking regime, such restrictions are likely to severely restrict innovation and the consumer benefits that will arise from the use of the data.

Rather, we recommend that consideration should be given to ensuring the regulatory regime is flexible and able to respond to how the Open Banking data is used – and consent gained - in practice. This could include empowering the ACCC to issue Rules relating to both the form of consent and, ultimately, the permitted uses of data obtained through Open Banking. One way of achieving this would be through the development of a set of standardised use cases and associated consents – providing certainty and clarity to both industry and consumers. While it might be argued that such standardisation might restrict innovation and restrict consumer choice, in reality it should be possible to categorise a wide variety of potential business models into a few generic use cases and consents. This may also prove to be a more effective way for industry to initially implement Open Banking; or be available on an optional basis so that businesses may choose a simplified form of accreditation based on those standardised use cases.

We set out some additional matters for consideration, and specific suggestions, in respect of *Recommendations 2.8, 4.5, 4.6 and 4.7* in *Annexure One*.

Interaction of Open Banking and Part IIIA Credit Reporting System

Open Banking has the potential to improve the responsible lending practices of credit providers, for example, by enabling better verification of a credit applicant's disclosed income and expenses. Credit providers will, with consent, be able to access the transaction records of an applicant, in a secure and efficient manner, to identify the income going into the account and the expenses coming out.

Open Banking will also have a role in credit decisioning that goes beyond the simple verification of the applicant's financial position. Credit providers are likely to use the Open Banking data more broadly to make better credit risk decisions.

First, the transaction data will not just provide evidence of how much the consumer spends, but also *where* and, by inference, *on what* the consumer spends their money. For example, the credit provider may see that an applicant is regularly withdrawing cash at ATMs that are located at gambling venues – which could indicate that the applicant has a gambling problem and is an unsuitable credit risk.

[2] We note that the Review refers to the consumer giving 'consent' to the exchange of their credit information with CRBs (see p.50 of the Review). This is incorrect. Part IIIA establishes the right of the CP to exchange information with a CRB if a consumer has applied for consumer credit, subject to the consumer being given the required notice. This business right cannot be withdrawn by the consumer.

Secondly, the credit provider will obtain the transaction history of the applicant's other existing credit products which could (subject to the data standards) include details such as the running balance of the credit product and the value of repayments required and made under the contract.

All of the above types of data are highly informative to credit providers when making credit decisions, however are currently prohibited from being shared in the Part IIIA credit reporting system.[3]

In addition (as noted above), Part IIIA and the CR Code strictly limits the use and on-disclosure of information shared through the Part IIIA credit reporting system. For example, a credit provider is not permitted – even if they sought the consumer's permission - to use any information obtained through the Part IIIA credit reporting system to offer any product to the consumer, other than the specific product that the consumer has applied for. Data obtained through Open Banking appears not to be subject to those restrictions (i.e. the credit provider may use the data for any purpose for which they receive consent).

To be clear, ARCA's position is that credit providers should have access to a wider range of data including balance, payments, and transaction level data to make better credit decisions. We have advocated for this in relation to broadening the range of data permitted under Part IIIA.

However, as a preliminary issue, the Review should clarify how Open Banking and Part IIIA interact as it currently appears that the intention is for Open Banking to remove the constraints in Part IIIA (albeit subject to the consumer consenting). If this is the case, it must be recognised that this will enable credit providers access to data, and permit use of that data, that has otherwise been denied or strictly limited under Part IIIA.

Nevertheless, ARCA considers that Open Banking will not operate as a replacement for the Part IIIA credit reporting system, and that the two systems will work together.

Importantly, the Part IIIA credit reporting system contains data on most credit active consumers in Australia – and businesses (subject to the requirements of Part IIIA and the CR Code) have a right to access this information in prescribed circumstances *without* consumer consent. This is in contrast to the Open Banking regime which will only have data for consumers who have provided, and who have not withdrawn, consent (noting our earlier comments in relation to such consent being a condition of the provision of the product or service).

In addition, even where a consumer has provided consent for a prospective credit provider to access their data held with existing credit providers, the prospective credit provider will need to access the Part IIIA credit reporting system to validate what accounts are held by the consumer as this is the only central repository of that information.

We set out some additional matters for consideration, and specific suggestions, in respect of *Recommendation 4.2* in *Annexure One*.

[3] It is important to note, however, that if the consumer applies to their own bank for credit, that bank is not prohibited from using the same types of information in their credit decision (subject to the requirements of the Australian Privacy Principles). Likewise, a credit provider could obtain access to this information by requesting the information directly from the applicants (potentially using screen scraping technology).

The Scope of Open Banking

Types of transaction data

We agree with *Recommendation 3*.2 that there should be an obligation to share all transaction data of the consumer. However, we note that additional work must be done to identify what precisely constitutes that data. While many of the use cases for Open Banking data are not yet known, it is important to have a clear idea of the *likely* use cases and ensure that the data made available will, at least, meet those purposes.

For example, as described above, it is likely that credit providers will use Open Banking data to supplement the Part IIIA credit information when making credit decisions. On that basis, it is important to ensure that the transaction data will include the relevant fields to enable that assessment. On this particular point, we note that ASIC in their submission listed the types of transaction data that should be included[4]. At a minimum, we agree with those suggestions. However, we strongly recommend that further consideration be given to the likely use cases for the data to ensure that the types of transaction data included in Open Banking meets those purposes.

We have set out some specific suggestions in respect of *Recommendation 3*.2 in *Annexure One*.

Standardisation of transaction data

As a related matter, the Open Banking regime should, in addition to the standardisation of the *process* for the exchange of data, aim for a level of standardisation of the transaction data actually being shared.

While the Review notes that the Standards should include *data standards* (in addition to *transfer standards* and *security standards*), the overall stated intent of the Standards is to allow accredited parties to 'efficiently connect and transfer'[5] data. However, ensuring that the data exchanged can be understood by data recipients is also necessary to realise the benefits of Open Banking.

For example, we expect that the requirement to share transaction data would include details of the merchant at which a purchase was conducted. Across the industry, there is no established standard by which that merchant is recorded in the bank's systems. So, when reporting the 'merchant details' through Open Banking, the bank could provide that detail in one of numerous different forms, including the business or corporate name of the merchant (either in full or abbreviated), a government identifier like the Australian Business Number (ABN), or an internally generated merchant identification number. Requiring the data recipient to interpret that data – even with the assistance of a middleware provider that is able to provide a standardisation service – is inefficient and, we expect in some cases, not possible.

Further, we caution against relying too heavily on middleware providers to undertake the data standardisation process.[6] As ARCA has observed in the credit reporting system, the use of

[4] ASIC submission, page 28 .

[5] Review, page 20.

[6] We expect that there will still be a role for middleware providers to provide standardisation – and value added – services. In the merchant example described, if the data standards require the data holder to disclose

competing proprietary data input standards can inhibit competition – because data recipients may only have scope to build their data transmission for one particular standard. This could lead to limited opportunities for data intermediaries, as data recipients will be more likely to use that intermediary who transmits the most data. In the credit reporting system, this issue has been overcome by the development of a common data standard (i.e. the ARCDS) which defines necessary data input characteristics.

ARCA's submission is therefore that industry should develop common data standards to ensure a level of consistency of data, so that data recipients are not overly reliant on middleware providers or are unable to interpret the data even with the assistance of middleware providers.

We set out some additional matters for consideration, and specific suggestions, in respect of *Recommendation 2.4* in *Annexure One*.

Additional detailed feedback

Our feedback in respect specific Recommendation is set out in *Annexure One.* In addition to the matters above, we have provided specific feedback is relation to:

- *Recommendation 2.7* – ensuring the accreditation requirement is not circumvented [See *Item 3* in *Annexure One*]
- *Recommendation 4.9* – allocation of liability [See *Item 11* in *Annexure One*]

If you have any questions about this submission, please feel free to contact me.

Yours sincerely,

Mike Laing
Executive Chairman

the ABN (as the description of the merchant), middleware providers will likely offer services to provide the name of the business (using the government databases) and details of the type of business engaged in by the merchant.

AUSTRALIAN RETAIL CREDIT ASSOCIATION

ANNEXURE ONE:

ARCA's Submission on Review into Open Banking in Australia – Final Report

	Review Recommendation	ARCA Comments	ARCA's Submission
1.	2.4 – Rules written by the ACCC	See *ARCA Submission – Industry's role in developing the Rules and Standards.* The drafting of the industry specific Rules will require a detailed understanding of the operation of the specific industry. This understanding is unlikely to be within the ACCC's experience. Under the *Privacy Act,* the Information Commissioner is permitted to appoint a 'code developer' to develop a code and, subsequently, apply to the Commissioner for registration of that code. This approach puts the industry's knowledge and experience to use to develop the detailed, industry-specific rules, while not detracting from the opportunity for all stakeholder groups to participate and be consulted during the process. The Explanatory Memorandum to the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012*, which introduced the concept of a 'code developer', notes (at page 36): *[Industry] control of the code making process would:* • *allow the industry to apply detailed knowledge of industry practices to determine the best procedures to*	The ACCC should be given the power to engage a 'Rules developer' (which would be a relevant industry representative) to develop the industry specific Rules, which would then be authorised by the ACCC. The industry representative engaged as the Rules developer would require a broad mandate from a wide cross-section of stakeholders, and would need relevant experience in the setting of industry standards. While we see that ARCA would have a role in this process, we are not suggesting that we take the lead.

		ensure practical compliance with the requirements of the Privacy Act • *provide the industry with the flexibility to review the Code and develop necessary changes to the Code (subject to OPC approval) as required by changes in industry standards; and* • *ensure the credit reporting industry adopts best standard practices which have been developed in consultation with all industry participants, improving the overall reliability of industry practices and enhancing the operation of the credit reporting system.* *The ability of the credit reporting industry to develop (in consultation with stakeholders, including consumer advocates) and adhere to a binding Code may assist the industry build greater trust by individuals in the operational standards and reliability of credit reporting practices.*	
2.	2.5 – the Standards	See *ARCA submission - The Scope of Open Banking (Standardisation of Transaction Data).* Also, we note that given the proposed reciprocity requirements, the Standards will need to accommodate data sets that may be significantly different to those held by ADI data holders. For example, ARCA is currently considering how the new-styled 'buy now pay later' credit products (such as Afterpay, Zippay) would be reported in the Part IIIA credit reporting system. While these are 'credit products' they are structured in different ways to a traditional credit product (e.g. some have no structured payment obligations) and there is even significant variation between the products on offer.	Industry should be required to develop common data standards to ensure a level of consistency of data, so that data recipients are not overly reliant on middleware providers or are unable to interpret the data even with the assistance of middleware providers. If using the UK Open Banking technical specification as the starting point for the Standards, input should be sought from the creators and users of the UK APIs on what works well, what doesn't and what they would do differently if they were designing the APIs today knowing what they now know. Given the different regulatory landscapes, consideration should be given to what additional or different APIs would be appropriate in the Australian market. The Standards should be developed in a way that is readable and understandable by all impacted industry participants; it is not ideal

			if the Standards can only be read by participants with a highly technical background. To the extent that this is not feasible, the Standards should be accompanied by plain English explanatory material. The Standards will need to accommodate the sharing of data by data recipients (due to the reciprocity requirements) that may be in significantly different form to that shared by ADI data holders.
3.	2.7 – accreditation	We see two ways for the accreditation process to be circumvented: • An unaccredited party could encourage a consumer to access their Open Banking directly for the purposes of passing that data on to the unaccredited business. • An unaccredited party could seek the on-supply of Open Banking data from an accredited party. Provided the accredited party obtains the consent of the consumer, it does not appear that this would be prohibited in the Open Banking regime. An unaccredited party that obtained access to the data in this manner would avoid the costs of accreditation, the additional privacy protections otherwise applicable to accredited parties and the reciprocity obligations under Open Banking - this last issue is also noted in Item 7, below. In respect of the second point, we note that the Review (at page 90) states: *As discussed in Chapter 4, customer-facing applications that receive information from a middleware provider would still require accreditation and liability would be assigned using existing legal principles.*	Consideration should be given to whether it is appropriate to impose restrictions on unaccredited third parties seeking to indirectly obtain access to Open Banking data. For example, unaccredited parties could be prohibited from: • Encouraging a consumer to directly access the Open Banking data for the purposes of passing that data on to the unaccredited business; or • Seeking the on-supply of Open Banking from accredited parties.

		However, it does not appear that Chapter 4 discusses this issue in detail.	
4.	2.8 – the accreditation criteria	We note that the Review rejected the idea that accreditation be based on specified 'use cases', on the basis that "consumers should be free to choose their own uses and seek value outside of that currently considered by industry or regulators" (page 24 of the Review). However, we note that the *optional* use of standardised use cases with accreditation based on that use case - and potentially combined with standardised consents - could encourage competition in the provision of simple services (using Open Banking). For example, if there is a simple form of a product comparison tool, providing a simplified and standardised accreditation and consent proposed based on that specific use case may encourage more service providers to enter the market.	ACCC should be given the *ability* to establish accreditation requirements based on standardised use cases (with, potentially, standardised consents).
5.	2.11 – remedies for accredited parties	The ARCA-developed PRDE includes detailed dispute resolution principles. These principles are based on the recognition that industry participants are most likely to identify potential non-compliance by other industry participants. As such, PRDE establishes a series of business-to-business rules that allow a credit provider (CP) or credit reporting body (CRB) that has identified potential non-compliant conduct (e.g. a failure to disclose all data that is required), to directly raise the concern with the CP or CRB that has allegedly engaged in the conduct. This process encourages the parties to resolve the issue in a quick and low-cost manner. If the dispute is not able to be resolved, the PRDE provides for an escalation process, including referral to an industry determination group and, ultimately, to an eminent person. The outcomes available include finding that there has been no non-compliant conduct, a warning to the non-compliant CP or CRB, a direction to a non-compliant CP or CRB to take certain action (e.g. staff	The Standards should include business-to-business rules that provide for a dispute resolution process similar to that contained in the PRDE, including: • An initial process that encourages resolution of the dispute between the data holder and data recipient. • An escalation process for disputes that are not settled between the parties. • An industry-based method of adjudicating disputes that cannot be settled between the parties • A range of remedies available to the industry-based adjudicator, including restricting or removing the accreditation of the non-compliant data holder, so that they may not receive data through the Open Banking regime for a nominated period. Any breach reporting obligation to the ACCC should not be triggered if the dispute is resolved between the data recipient and data holder within an initial timeframe. Likewise, there should not

		training or to provide evidence of compliance) or to limit the data that the CP or CRB can share through the credit reporting system. The rules establish a clear timeframe for the consideration and escalation of the dispute.	be a breach reporting obligation if the adjudicator finds that the data holder has not engaged in non-compliant conduct.
6.	3.2 – transaction data	See *ARCA submission - The Scope of Open Banking (Types of transaction data).*	The types of 'transaction data' to be included in Open Banking should be carefully considered to ensure that they meet the needs of the likely use cases for that data.
7.	3.9 – reciprocal obligations in Open Banking	The Review proposes that data recipients be subject to a reciprocity obligation. As noted in Item 3, there are incentives for businesses to avoid both the accreditation process and the reciprocity obligations. In Item 3 we have recommend that the Review consider limiting the ability of unaccredited parties from seeking indirect access to Open Banking data. However, even if this is done, unaccredited parties may still receive the *benefit* of the data, without actually receiving any of that data - therefore, avoiding the reciprocity obligations. For example, a credit provider may engage an accredited party to access the data for the purposes of creating a 'credit score' that is given to the credit provider to assist with their credit decision. As that credit provider has not received any of the data obtained through Open Banking, they would not, despite getting the benefit of the data, be subject to the reciprocity obligations. As a separate matter, we note that the reciprocity obligation appears to be unrestricted – that is, provided a data recipient receives some Open Banking data, that data recipient is then required to make *all* their transaction or transaction-like data available. In contrast, under the ARCA-developed PRDE, the	The Rules relating to reciprocity must be carefully considered to ensure that they set out the appropriate participation levels, and exceptions. Consideration should be given to: • Extending the reciprocity requirement to entities that receive the benefit of Open Banking data (e.g. through the use of information derived from that data), even if the entity does not receive the actual consumer data. • Allowing the Rules to permit a restricted reciprocity obligation for non-ADI data recipients in appropriate circumstances, including if the ACCC has provided for a simplified accreditation based on a standardised use case.

		reciprocity obligation allows credit providers to choose to receive a more limited range of data, while only being obliged to supply the same level of data. While we recognise that ADI data holders will be required to supply all data in respect of the relevant banking products, requiring this same level of data sharing from smaller, non-ADI entities may be counterproductive and discourage *any* level of participation by those entities. As noted in Item 4, we consider that there is merit in allowing simplified accreditation based on standardised use cases. As part of the simplified accreditation process, we would suggest that this also permit a more limited version of reciprocity that would permit data recipients (other than ADIs) to obtain a subset of available data, and only be required to make available an equivalent subset of their data. This would encourage more participants to offer services based on the standardised use cases.	
8.	4.2 – modification to privacy protections	See *ARCA submission - Interaction of Open Banking and Part IIIA Credit Reporting System*. In addition: • It is possible that a data recipient acting as an intermediary between a credit provider and another credit provider would be considered as acting as a *credit reporting business* under *section 6G* of the *Privacy Act* and, therefore, subject to the restrictions and requirements of *Part IIIA*. • *Table 4.1 Modifications of privacy protections for Open Banking* sets out the required changes to the Australian Privacy Principle. In addition to the APPs, *section 21B* of the *Privacy Act* imposes additional notification obligations on a credit provider in respect of 'credit information' (as that term is used in Part IIIA). Those requirements will	The Review should clarify how Open Banking and Part IIIA interact, including whether it is the intent of Open Banking to permit CPs (subject to customer consent) to obtain additional types of data, potentially for purposes not permitted by Part IIIA and the CR Code. In particular, the Review should clarify whether, and how, *section 6G* and *section 21B* of the *Privacy Act* should be amended in response to Open Banking.

		also need to be reviewed in light of the introduction of Open Banking.	
9.	4.5 – customer control; 4.6 – single screen notification	See *ARCA submission – Consent and Consumer Protection – and the need for certainty for industry*.	Consideration should be given to empowering ACCC to issue Rules to (for example): • Monitor the types of use cases that develop and the associated consents that are being used • Develop standardised consents for standardised use cases, including simplified consents for low risk use cases (such standards consents would provide the benefit of moving the focus away from competition around which business can develop the most expansive consent process) • Impose minimum consent requirements for higher risk use cases • In limited circumstances, and subject to appropriate consultation, prohibit certain use cases • Require reporting by data recipients on consumer outcomes resulting from use of Open Banking data (e.g. pricing, access to products or service) • Permit additional use cases not otherwise covered by the original consent (subject to an assessment of consumer benefit) – this would enable innovation in use cases, in appropriate circumstances, without the cost of seeking additional consents. Any such Rules imposed by the ACCC on the consent process should be informed by behavioural economics.
10.	4.7 – joint accounts	ARCA considers that the analogy drawn between the transfer of money from a jointly held account, and the transfer of data from such an account is not appropriate. This analogy does not recognise that in the case of money, the transfer makes the money unavailable to the other joint account holder. This is not the case in respect of a transfer of data; the data remains for the other joint account holder to share.	ARCA recommends that the proposed approach to jointly held accounts be reconsidered, such that: • any joint account holder may give access to data in respect of that account; and • one party cannot terminate a data sharing arrangement initiated by another joint account holder.

		A more fitting analogy is to compare the Open Banking situation to a joint account holder's right to access their transaction history through periodic statements. For example, each joint borrower under a loan regulated by the *National Credit Code* must receive a statement of account unless they provide a written instruction otherwise (where such notice can be withdrawn at any time). Further, we consider that this approach may have unintended consequences: • An account holder may take out a product or service, independently of the other joint account holder, where the provision of that product or service is dependent on the continued access to Open Banking data in respect of the joint account. Under the current proposal, the other joint account holder would have the ability to terminate the Open Banking access and interfere with the consumer's enjoyment of the product or service. • If access to data on a jointly held account is made more complicated by the fact that the account is 'both to sign' this may act as an incentive to change the account authority to 'either to operate' (and put the account holders at risk that another account holder could inappropriately withdraw funds).	
11.	4.9 – allocation of liability	The principles for a comprehensive liability framework (Table 4.2, page 66) suggests that a bank should be liable to the customer if it mistakenly shares that customer's data with an accredited party. The principles do not suggest, or recognise, any steps that the bank can take to mitigate the risk of customer loss resulting from that mistake. As a separate matter, *Recommendation 4.9* suggests adopting the principle that participants "are liable for their own conduct, but not the conduct of other participants". However, it also recognises the	At a minimum, the data accreditation process should impose obligations on the data recipient to destroy data if advised by the data holder that it has been incorrectly disclosed. When so advised, the data recipient should indemnify the data holder for further unauthorised use (resulting from the data recipient's failure to destroy the data). Consideration should also be given to whether the bank can reduce its direct liability to the customer. For example, this could mean that the bank should not be liable for the loss if it has advised the customer of the mistake and has suggested reasonable steps for the

		use of intermediaries (i.e. 'middleware providers') in Open Banking. While liability as between the intermediary and the provider of the customer-facing application is suggested to be assigned "using existing legal principles" (page 90), this statement is not expanded upon in Table 4.2. Given the potential range of commercial relationships that may exist between intermediaries and the final users of the data, we suggest that the Rules establish the principles. For example, we note that it could be possible for the final user of the data to establish a process under which the consumer appoints the intermediary as the consumer's own "agent", so that the final user avoid liability for that intermediary's mistakes.	customer to take to avoid loss, and the customer has unreasonably failed to take those steps. The Rules should set out in more detail how liability will be assigned between intermediaries and the final users of the data, which may need to alter the existing legal situation.
12.	6.1 – the Open Banking Commencement Date; 6.2 – phased commencement for entities	See *ARCA submission – Timing*. Beyond the technical work to provide for the exchange of data, there is a significant amount of work to develop an appropriate regulatory regime, and data standards. We believe that the 12-month implementation timeframe proposed in the Review is ambitious.	The timing of implementation should recognise the amount of work required.