Australian Banking Association

21 May 2020

Secretariat
Inquiry into Future Directions for the Consumer Data Right
The Treasury
Langton Crescent
Parkes ATC 2006

By email: data@treasury.gov.au

Dear Mr. Farrell

Inquiry into Future Directions for the Consumer Data Right

The Australian Banking Association (ABA) welcomes the opportunity to make this submission to the Inquiry into Future Directions for the Consumer Data Right (the Inquiry). The ABA supports the ongoing development and expansion of the Consumer Data Right (CDR).

The ABA approaches this discussion with a deep appreciation of the effort, skills and considerations required to enable a safe, secure, and smooth expansion of the CDR. As the first sector to launch with Open Banking, the banking industry has contributed significantly to operationalising the CDR vision through expertise within the sector as well as providing the Open Banking systems through which the first consumer data will flow in the CDR.

ABA recommendations

The detailed submission is annexed however, the recommendations contained within are:

Recommendation 1: The ABA supports recommendation 6.6 of the 2017 'Review into Open Banking (the Farrell report) – giving customers, choice, convenience, and confidence' which noted that a 'post-implementation assessment of Open Banking should be conducted… approximately 12 months after the commencement date and report to the Minister with recommendations.' The commencement date of Open Banking being that date when the final phase of Open Banking under the current policy is implemented into the live environment.

Recommendation 2: The ABA recommends that the development of innovative services using CDR and Open Banking not solely be subject to mandated compliance dates. Business strategies and not regulatory intervention should drive innovation through the CDR.

Recommendation 3: The Inquiry should set practical expectations for consumer switch propensities which is based on a sound understanding of consumer behaviours and consumer adaptation to a new technology and new service models over time.

Recommendation 4: Consent types and levels must:

(a) be appropriate to the level of risk and concern held for that data;

(b) be appropriate to the type of use cases to which the data will be applied;

(c) give consideration to the build complexity to manage the consents.

Recommendation 5: Voluntary data not to be subject to a predetermined standard.

Recommendation 6: The ABA supports the use of a tiered accreditation model which is based on the risk profile of the activities being considered. However, there should be no relaxation in the Open Banking obligations for data security, privacy, and consent.

Recommendation 7: In considering how write access may be introduced the Inquiry should closely example and provide direction for:

(a) The development of a definition of write access. This will also ensure consistent language, noting the language differences in the Issues paper between opening an 'account' and managing a 'product'.

(b) Legal responsibilities of data holders and third parties (data recipients) in respect to transactions and data created and transferred through a write access process.

(c) Scoping the relevant APRA and ASIC instruments, and the relevant AUSTRAC obligations under AML/CTF legislation to determine which aspects of these requirements can no longer be actively managed by the banks under write access and to determine an appropriate process for the updating of the relevant instruments and legislation.

(d) A payments initiation feature within the CDR must be based upon and subject to the existing governance processes of the chosen payments scheme(s). The ABA does not support the establishment of a new payments mechanism for the CDR.

(e) To consider other functions and features that may support a safe execution of write access including: digital Identity, electronic contracts and mortgages.

(f) Consumer consent processes and consumer recourse to data recipients.

Recommendation 8: In extending the CDR, a detailed consideration of the role of banking regulators (RBA, ASIC, APRA, AUSTRAC) and others such as payments governing bodies, and complaints management bodies should be undertaken to ensure a continuation of those governance arrangements under the CDR. The CDR should not be developing new banking governance structures where they already exist.

Recommendation 9: In respect to consumer protections:

(a) Consideration should be given to consumer protections, and whether these should be ecosystem-wide protections, overseen by the CDR governing body to prevent offerings that would exploit vulnerable customers.

(b) The government has a role to play in leading education campaigns to raise data literacy/CDR understanding across all consumers and also to focussing on vulnerable cohorts.

(c) There should be incentives to encourage the development of propositions that benefit vulnerable consumers and provide compelling use cases to manage their financial data and protect their financial wellbeing.

Recommendation 10: All participants who are prepared to use consumer data via the CDR regime should be required to reciprocate, irrespective of whether those entities are within a designated sector. The principle of reciprocity will ensure all participants are incentivised to deliver the right outcome for consumers.

Recommendation 11: This review to consider current governance arrangements of the CDR to create a stand-alone semi-government body which is:

(a) A single point of accountability.

(b) An entity that has human resources and funding capability to deliver such a significant economy-wide IT infrastructure project.

(c) An entity that can manage the complexity of such a build to ensure greatest possible commercial viability of that infrastructure. Including the undertaking of an extensive education programme for Australian consumers.

(d) Responsible for the end to end security of the ecosystem.

Recommendation 12: The establishment of a centralised CDR cyber-security capability, within the CDR governing body, which is separate to the internal security capabilities of the CDR. The centralised capability would be involved in intelligence gathering and coordinating responses to incidents and data breaches.

Recommendation 13: A comprehensive consumer government education programme to be undertaken in respect to consumer privacy rights under both the CDR Privacy Safeguards and the Australian Privacy Principles as a mechanism for engendering consumer confidence and trust in the CDR.

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.

The ABA thanks you for the opportunity to make this submission. Please contact me if you would like to discuss any aspect of this submission.

Kind regards,

Emma Penzo
Policy Director

Australian Banking Association

Inquiry into Future Directions for the Consumer Data Right
ABA submission

Australian Banking Association

1. Overview

The ABA supports the ongoing development and expansion of the Consumer Data Right (CDR) as it formalises the Australian data sharing market. However, it is important that all stakeholders involved in the establishment of the CDR – government, regulators, data holders, and data recipients – have a common understanding of the growth cycle and adoption trajectory of new developments. The ABA notes the following as important elements for all participants to be cognisant of in planning for the future expansion of the CDR:

It takes time to build and implement the systems infrastructure of the CDR: The complexity of banking in terms of product features, customer account structures, legislative and regulatory requirements, and organisational complexity means that it will take years to scope, build, test, and deploy the systems so that banking customers can undertake their banking activities safely in the live data economy.

It takes time to develop and mature a new market: The CDR, as the marketplace for data, will take time to develop and mature. It takes time for customers to develop familiarity, trust, and proficiency in the new marketplace. It also takes time for market participants to identify new and innovative use cases.

It needs to operate in lockstep with the real economy: The CDR could become a critical mechanism by which commerce is undertaken in Australia. In the meantime, it must operate in parallel with the real economy. This means that the rules which govern the operation of sectors in the real economy need to continue to operate within the CDR. A misalignment with the governance rules between the CDR and the real economy in the banking sector will create arbitrage opportunities which will be detrimental to consumer protections which are in place outside of the CDR.

Given this understanding, the following responds to each of the sections of the Inquiry into Future Directions for the Consumer Date Right, Issues Paper, March 2020 (the Issues Paper).

2. Achieving the vision of the CDR

The ABA supports the intention of the Inquiry: to examine ways in which the CDR can be extended as a key supporting infrastructure of the digital economy.[1] The banking industry, as the first to launch within the CDR, has contributed significantly to operationalising the CDR vision through the human capital expertise within the sector (product, policy, legal, privacy, IT technical, project delivery etc) as well as providing the Open Banking systems through which the first consumer data will flow. The banking industry approaches this discussion with a deep first-hand knowledge of the effort, skills and considerations required to enable a safe, secure, and smooth expansion of the CDR.

However, the ABA supports recommendation 6.6 of the 2017 'Review into Open Banking (the Farrell report) – giving customers, choice, convenience, and confidence' which noted that a 'post-implementation assessment of Open Banking should be conducted… approximately 12 months after the commencement date and report to the Minister with recommendations.'[2] The report noted that the 12-month post implementation review was important because 'this will provide sufficient time for the major behavioural response of the reforms to be observed.'[3] The ABA takes the commencement date of Open Banking being that date when the final of the current phases is implemented into the live environment.

The ABA acknowledges that the *Treasury Laws Amendment (Consumer Data Right) Act 2019* requires the Minister to commission an independent review of the Act which must report by 1 July 2022. This review could be brought forward, to also include a 12-month post implementation review of the CDR.

Whilst international comparisons are useful for considering the potential extension pathways of the CDR, the Australian Open Banking development has unique features, such as the breadth of product offering in the launch phases, which ought to be taken into consideration. Further, without an

[1] Inquiry into Future Directions for the Consumer Date Right, Issues Paper, March 2020 p1 (herein 'Issues paper')
[2] Farrell Report p.107
[3] Farrell Report p.107

operational Australian Open Banking system, there is a lack of local data and actual case studies which can evidence the experience of Australian consumers, data holders, data recipients and the performance of the ACCC's register. Therefore, suggestions for extensions to the CDR will largely be conceptual or extrapolations from international experience.

The ABA's experience in the operationalisation of the first stage of Open Banking is that this initial level of data sharing has involved significant complexity. The extensions envisaged in the Issues paper would introduce further complexity to the Open Banking build. Some of the build, the rules and the standards will need to be created anew to ensure that the security and privacy standards which are in place for the current features of Open Banking will withstand the demands and complexity from additional functionality. The time required to get this right will be significant to ensure the data security and financial security of banking customers. It is important that appropriate build and testing timeframes are factored into live date expectations.

The ABA understands the desire for accelerated delivery for many of the features under consideration by the Inquiry. However, based on the banking industry's extensive experience to date in operationalising Open Banking to date, accelerated timelines without due consideration of complexity, consumer experience needs, security and privacy impacts will impact upon magnitude and timeliness of consumer up-take of the CDR. Throughout this submission, the ABA recommends the Inquiry undertake 'deep dives' into areas of complexity. Where the appropriate level of detail cannot be attained through the Inquiry, consideration should be given to additional topic-specific reviews.

Recommendation 1:

The ABA supports recommendation 6.6 of the 2017 'Review into Open Banking (the Farrell report) – giving customers, choice, convenience, and confidence' which noted that a 'post-implementation assessment of Open Banking should be conducted… approximately 12 months after the commencement date and report to the Minister with recommendations.' The commencement date of Open Banking being that date when the final phase of Open Banking under the current policy is implemented into the live environment.

3. Future role and outcomes of the Consumer Data Right

The ABA recognises the opportunities for innovation which will come through the CDR. There is a distinction between introducing the infrastructure which will enable innovation and regulating or compelling innovation.

Open Banking broke ground and established the infrastructure required for a data sharing market in Australia through the CDR. Open Banking will be the first sector in the data economy and the ABA recognises the potential for innovation which this core infrastructure can bring to the Australian economy over the medium to long term.

However, commercial innovation as envisaged in the Issues paper cannot continue to be driven by regulatory compliance. Rather than mandated compliance dates for future Open Banking developments, participants should be given optionality in respect to how deeply their business engages with the CDR. Market dynamics have traditionally operated based on competition which encourages innovation.

This view is supported by the ODI Fingleton Post Implementation review which noted:

> 'Not all of the areas where we believe improvements are required should necessarily be mandatory for banks to provide for free to customers and TPPs. For some additional services, it may be useful to have standards set uniformly across the market, but for banks to contract privately with TPPs wishing to use the

service. This could increase the incentives for banks to develop their offerings further.'[4]

Recommendation 2: The ABA recommends that the development of innovative services using CDR and Open Banking not solely be subject to mandated compliance dates. Business strategies and not regulatory intervention should drive innovation through the CDR.

4. Switching Behaviours

The Inquiry has asked for comment on the role of the CDR in overcoming behaviours and regulatory barriers to switching between products and providers.[5]

Consumer switching behaviour is a complex and nuanced dynamic. To enable safe switching for consumers under the CDR, appropriate controls will need to be introduced to manage the combination of read and write access.

To date, the discussion surrounding Open Banking's role in facilitating switching has predominantly focussed on 'value', especially in respect to better priced products. However, a Deloitte report[6] points to many other attributes which need to be present for customer switching behaviour to increase. Deloitte identified five areas which are critical in supporting customer switching. These are trust, privacy, engagement, value propositions, and customer propensity for change.

The CDR design and rollout, and customer education programmes need to address each of these areas as they drive the scale and uptake of Open Banking.

Trust: The Deloitte report identifies three types of trust important to banking customers: prudential, information; and relationship trust. For consumers to consent for their data to flow from data holder to data recipients the level of trust in the data recipient needs to be as great or greater than the customer's trust in the data holder. Customers trust their banks to protect their money (prudential), and to keep their transactions secure (information). Where a data recipient is not subject to the same prudential and security requirements, trust in the CDR will be impaired.[7]

Therefore, a carefully designed accreditation model must be implemented. One measure will be a robust accreditation process and a tiered accreditation model that reflects the risk profiles associated with expanded read and write activities, without relaxing the existing obligations concerning security, privacy, and consumer consent.

Privacy: Customers need to know with transparency how their information will be used, and they need to be able to provide and rescind their consent for the use of their data. The degree of confidence of consumers in respect to Open Banking is yet to be determined as the ecosystem has not yet been launched. However, customer consent arrangements will be pivotal to get right.

Engagement: The Deloitte report identifies financial literacy, capability, and consciousness as parameters of engagement. A proxy for engagement is financial capability. The greater a consumer's financial capability, the greater will be their engagement in financial decision making.

A recent RMIT report[8] identifies several factors which may be determinants of financial capability. These include psychological factors such as confidence; external factors such as cultural norms; and the need to improve cut-through with financial education programs.

These factors are determinants of financial literacy currently. Open Banking as a data innovation will necessitate additional levels of education to bolster data financial capability in the Australian population.

---

[44] John Fingleton, 2019, 'Open Banking, Preparing for lift off' https://www.openbanking.org.uk/wp-content/uploads/open-banking-report-150719.pdf p38
[5] Issues paper p5
[6] Deloitte, 'Open banking: switch or stick. Insights into customer switching behaviour and trust' October 2019 https://financialcapability.gov.au/files/open-banking-switch-or-stick-insights-into-customer-switching-behaviour-and-trust.pdf
[7] Refer to section 5 'Tiered Accreditation' and recommendation 6
[8] Russell, R., Kutin, J. & Marriner, T. (2020) Financial Capability Research in Australia. RMIT University. https://financialcapability.gov.au/files/financial-capability-research-in-australia.pdf

Value: The Deloitte report notes that value is not just about pricing value but also convenience value and problem solving value. The latter value requires new solutions to existing or emerging consumer problems which may be delivered through the CDR. Such propositions are subject to strategic business cases by organisations and will take research and time to emerge.

***Customer profile*:** The Deloitte report identifies typical switchers as being tech savvy, highly educated, with high incomes. This suggests that Open Banking will be appealing to a small segment of the population in the early to medium term. This view is supported by a report by Accenture[9] which identified three banking customer segments: the "nomads" who are digitally savvy and not committed to traditional banking providers; "hunters" who are price sensitive and move for better priced deals; and "quality seekers" who are concerned with quality service and data security.

Irrespective of how the Australian banking market is segmented, the indications are that initially there will be a small segment of early adopters who use the CDR. The ABA's expectation is that a data innovation as significant as the CDR requires time for the population to firstly understand, then trust and then use.

Further, switching levels in isolation may not be an accurate measure of the full benefits that customers may receive from participating in Open Banking. This is because customers may utilise Open Banking to source alternative offers but may choose to stay with their existing provider. Therefore, a measure of switching in isolation will not capture that customer's benefit derived from Open Banking.

Recommendation 3: The Inquiry should set practical expectations for switch propensities which is based on a sound understanding of consumer behaviours and consumer adaptation to a new technology and new service models over time.

5. Read access

The Inquiry asks for consideration on options to extend read access along several dimensions: standardised taxonomy; consumer tracking of all consents; standardisation of voluntary data sets; tiered accreditation. Each will be addressed separately however any extension to read access beyond that which has currently been devised for Open Banking will involve additional complexity to the design and build of Open Banking.

A taxonomy for standardised language for consents

The Issues paper invites comment on the potential to develop a 'consent taxonomy' which can be standardised across sectors and providers.

Open Banking consent taxonomy

The ABA supports a consent taxonomy within Open Banking as it will enable more detailed consents to be provided by customers thereby providing customers with more control. The consent arrangements within Open Banking under read access has involved a lengthy process where customer experience (CX) tests have been undertaken to determine preferred levels of consent, expected flows for the provision of consent, as well as the granting, revoking and extending of consent. These tests have been performed for individual account holders as well as joint account holders. The joint account holder requirements are more complex than those for the individual account holder.

Such requirements have resulted in technical standards and systems builds of very significant complexity.

Within Open Banking, the common consent taxonomy, supplemented by a technical solution that allows customers to provide more granular consents should address privacy protections as it will enable greater consumer control over the data they choose to share (e.g. only sharing withdrawal information

[9] Accenture (2017) 'Beyond Digital: How can banks meet customer demand?'p6. https://www.accenture.com/_acnmedia/Accenture/next-gen-3/DandM-Global-Research-Study/Accenture-Banking-Global-Distribution-Marketing-Consumer-Study.pdfla=en

on an account, or only sharing deposits from a particular person, or during a date range set by the consumer). This aligns with the principle of data minimisation by allowing only the necessary data to be shared.

Multi-sector consent taxonomy

Given the higher level of concern held by consumers in respect to their banking data security and privacy, a multi-sector common taxonomy could be challenging because (a) all data is not equivalent and (b) it may introduce far more significant privacy risks which will need to be managed (c) it may result in less control for the consumer (d) legacy systems will need to be considered.

Data Equivalence

'Data equivalence' is implied in the concept of a common taxonomy. That is, that a consent provided by a customer for the sharing of their data means the same thing across all sectors of the economy.

All data is not necessarily equivalent according to the Australian public. Survey data released by the Office of the Australian Information Commissioner (OAIC)[10] showed that of all data types, Australians were most reluctant to share their banking information with government and business. Forty-two percent of Australians felt that their financial data was private (Figure 1).

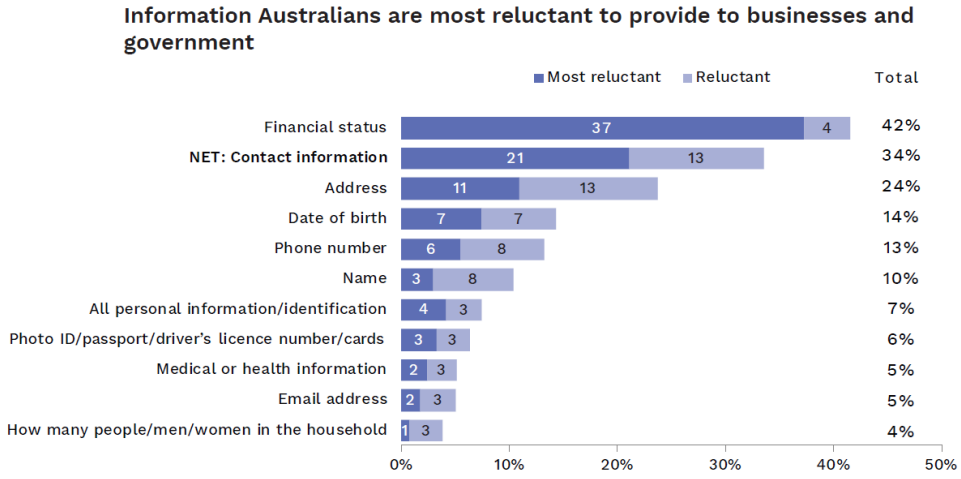

Figure 1: Source OAIC 2017 p6

The reasons for their reluctance to share financial data were insightful. Australians are concerned for the potential for financial loss, privacy, potential for misuse, and potential for becoming victims of cybercrime (Figure 2).

[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

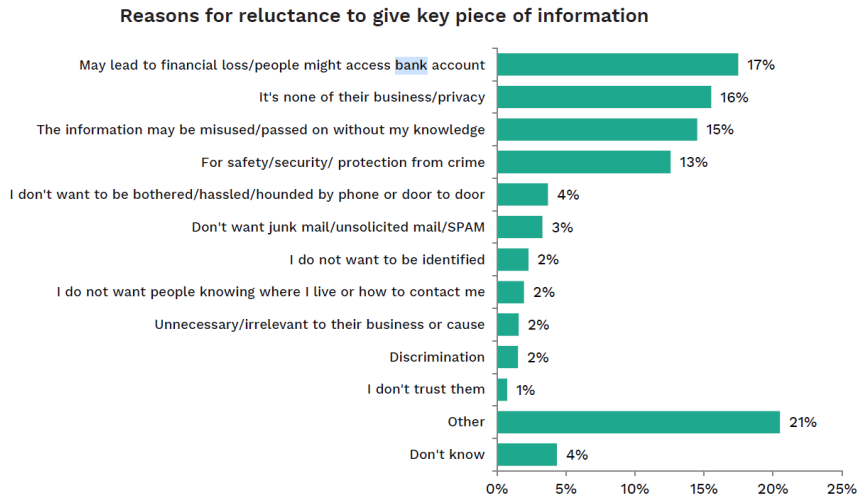

Figure 2: Source OAIC 2017 p7

Therefore, the risk of a common consent model is that the consent is developed at such a 'high level' that it does not provide the consumer the level of control over their data that they require in order to have trust that they can control how third parties will use that data.

Common consent enables 'super' data recipient models

A common consent protocol will enable the establishment of 'super' data recipient models. Take the case of a data recipient which can compile a customer's banking, telecommunications, energy data, and search engine search history into one place. The data recipient will have the potential to profile the customer to a level of detail which currently is not possible. The increasing sophistication of Artificial Intelligence software will enable deeper insights into a consumer's preferences. It will be possible for a 'super' data recipient to know more about the predispositions and propensities of the consumer than the consumer would know of themselves. Data recipients will be able to project the customer's future actions and make pre-emptive offers. Leaving the ethics of such use cases to one side, such use of data will require much greater levels of disclosure to the customer and appropriate levels of consent and accreditation.[11]

Common consent diminishes consumer control

A common consent taxonomy may not be empowering for consumers. The risk of a common consent model is that the consent is developed at such a 'high level' that it does not provide the consumer the level of control over their data that they require in order to have trust that they can control how third parties will use that data. It also prohibits data holders and data recipients from responding to consumer demand for more granular levels of consent in their offers.

Legacy systems

The prevalence of legacy systems with long lives, legacy data stores, and retooling expenses, makes it a significant challenge to introduce common data standards across sectors. Detailed consideration of the viability of a common taxonomy should include consultation with technical experts in data science and data governance within and across sectors.

If a standardised CDR-wide consent taxonomy is required, it should be positioned at the minimum standard and enable participants to offer finer levels of consent as needed for the use cases.

[11] This assumes the consumer has a solid level of financial and data literacy with no vulnerabilities. See section 8.

Recommendation 4: Consent types and levels must:

(a) be appropriate to the level of risk and concern held for that data;

(b) be appropriate to the type of use cases to which the data will be applied;

(c) give consideration to the build complexity to manage the consents.

Consumer tracking of consent management

Consent management and tracking in Open Banking is particularly complex. Facets of consent which the banking industry has worked to define with the Australian Competition and Consumer Commission (ACCC) and the Data Standards Body include:

- Basic consent where there is one consent per data recipient
- Concurrent consent where this is more than one consent per consumer per data recipient
- Joint account management where there is consent between two account holders for the sharing of data.

Yet to be defined are consents for business accounts. These arrangements will be particularly complex because of the 'multi-user' nature of account authorities due to company governance arrangements.

Consent management tracking at the consumer level which centralises all consents cross-sector and potentially cross-consumer-business account operator/holder is not in keeping with the existing model of distributed consent. Instead, resolving the complexities of consent in the full implementation of Open Banking so that the distributed consent model meets consumer user requirements should be the priority.

Voluntary data sets

Given the newness of the Open Banking APIs, the convergence towards standardised voluntary data sets is yet to be tested in the market. Standardisation of voluntary data is a pseudo regulation and it may create additional barriers to providing that data. For example, if it is not possible to align to the standards the data holder may choose to not provide the voluntary data. Further, the voluntary data may have been deemed voluntary because it is not readily standardisable due to legacy systems and legacy data stores.

Recommendation 5: Voluntary data not to be subject to a predetermined standard.

Tiered accreditation

The ABA supports a robust accreditation process and a tiered accreditation model that reflects the risk profiles associated with expanded read and write activities, without relaxing the existing obligations concerning security, privacy, and consumer consent. The primary consideration of the future CDR regime must be ensuring that consumer trust and confidence in the regime is not reduced through a weakening of the consumer protection mechanisms in the CDR framework.

Accreditation levels should be commensurate with the overall risk profile of the proposed participation model of the data recipient. In order to form a view of the overall risk profile the following elements should be considered:

(a) the data – Open Banking entails the transfer of banking data and personal data which requires a high duty of care.

(b) read versus write access – write access will require significant upgrading of security measures relative to read access due to the additional access it provides.

(c) resources of the data recipient – the data recipient can demonstrate its capacity to manage the requisite security and privacy requirements in terms of its human, financial, and technical resources, including its ability to meet claims in the event of breach.

Australian Banking Association

Recommendation 6: The ABA supports the use of a tiered accreditation model which is based on the risk profile of the activities being considered. However, there should be no relaxation in the Open Banking obligations for data security, privacy, and consent.

6. Write Access

Significant complexity

The Issues paper notes several 'write' use cases which third parties may be able to undertake at the direction and consent of the customer. These include change or add data about a customer; apply for products; open new accounts; manage products; change products; close products.

Examples in the context of banking are represented in the table below:

Proposed third party actions	Credit card example
Change/add data about a customer	Change of email address
Apply for products	Apply for a credit card
Open new accounts	Open a subsidiary account on an existing credit card
Manage products	Apply for a credit limit increase
Change products	Apply to change to a different credit card product
Close products	Request to close credit card
Initiate payments	Make a purchase on behalf of a customer using the customer's credit card credential. Switch accounts by transferring account balance from Bank 1 to Bank 2 and closing the account with Bank 1.

The above examples are suggestive of a 'shadow' banking system, where a third party, that provides banking services, such as advice, support, and account maintenance, acts on behalf of the consumer. Several observations are warranted:

- ***Third party 'bankers'***: The third party would need to demonstrate the capability of a competent banker. One who is capable of interceding on behalf of the customer and making recommendations in respect to which credit card to apply for as well as credit limit. Additionally, they would need to ensure that income, expense, and other information was accurate and true.
- ***Security & Privacy***: Much of the data which the intermediary will collect is subject to significant security and privacy protocols by banks, the third party would need to demonstrate functional equivalence.
- ***Consents***: There is a significant assumption that the consumer consents required by third parties for write access are simple to code, simple to attain from the consumer, simple to explain to the consumer; and that ultimately the consumer understands the consent that they are providing. Further, there is an implicit assumption that banks are to accept that the third party's consents can be relied upon.
- ***Fraud detection***: A large element of fraud detection is through the tools a user interacts with to contact the bank (e.g. internet banking). Third party involvement in the process may mean that banks will no longer be able to undertake such detection or the detection may be less effective.

- ***Liability***: The liability regime for the banks would need to be considered. Banks cannot be held accountable for the information provided, and actions taken, by third parties under consumer consent. If the efficiency and innovation ambitions for write access is to eventuate through the provision of some banking services through non-bank third parties that liability needs to transfer to the third party. For example, ASIC could consider its Responsible Lending requirements considering the third party's activities in the lending process.

These examples are a brief demonstration of the potential level of complexity which will underpin the development of features for write access in banking. They are high level and incomplete for the chosen credit card product and do not reflect the degree of complexity arising if the entire suite of phase 1, 2 and 3 banking products were to become subject to write access.

The CDR should allow data holders to process any write access requests in line with their existing approach for such requests. Further, personally identifiable information should be excluded due to security, fraud, and privacy risks. In respect to personally identifiable information banks are legislatively obligated to fulfil Know You Client obligations and Verification of Identity obligations. Write access will need to preclude third parties from access to these data elements.

An accelerated implementation of write access in Open Banking could create an unregulated digital banking shadow system not supported by the existing liability regime. Further consideration should be given to tiered write access for data recipients.

Payments

Consumers currently have several ways of initiating payments (from cards in-store, in-app, using a wallet or online, to cash, to direct debits, to online banking with pay anyone, including real-time Osko and BPAY). The current payments governance protocols and fraud controls provide considerable protection for consumer funds. These governance arrangements have evolved as knowledge of the risks and available controls has grown. The governance arrangements of payments schemes understand the trade-off between enhanced consumer functionality against risk. For example, as the internet evolved banks (2nd parties) began offering payment initiation from consumers (1st parties). Initially internal transfers between accounts, then BPAY evolved from a telephone banking service to online banking, and then as risk controls improved banks introduced Pay Anyone. Importantly, today not all Australian banks accept payment instructions for all forms. The only current mandated form of acceptance of a payment instruction is a cheque, via the *Cheques Act*, where banks must honour (or dishonour in some circumstances) "an instruction in writing" from a customer.

In light of that history, if the intent for write access is to mandate that all banks (2nd party) must honour a payment instruction from consumer (1st party) via a 3rd party for credit to a 4th party (payee) it would be an unprecedented large step into an unknown risk environment.

Other considerations

Digital Identity

COVID-19 has proven the business case for the use of digital identities in the public and private sector. Having a robust way of onboarding and identifying customers within an organisation and across organisations is key to the success of a future CDR. Customers need to be reliably identified between organisations to ensure the right customer data is provided to a third party, an instruction is applied to the right customer account or a customer's consent is recorded and implemented.

Trust is key to developing a marketplace for data under CDR, and an effective digital identity service is fundamentally predicated upon trust. No customer identification solution is without risk for banks and customers, however a digital identity service that meets the banks and customers' requirements can significantly mitigate the risk of misuse, loss or unreliability of data, which in turn can erode customers' trust in the CDR.

An effective digital identity service needs to be supported by appropriate rules, governance, technology, and legal frameworks. The right settings for these frameworks are being considered by a number of public and private sector parties.

The Australian government has introduced the trusted digital identity framework, and there is an existing emerging industry surrounding digital identity services with the potential for it to support the CDR. A consultative approach should be undertaken with developers of digital identity frameworks with open standards encouraged within the CDR, so the CDR does not mandate standards which may not be fit for purpose in the future and could deter innovation.

Electronic signing of documents and electronic mortgages, electronic witnessing

The ABA considers e-transactions reforms are a precondition of implementing write access under the CDR. For example, to enable write access for business accounts and mortgage accounts legal certainty is required that a document can be created, stored, signed, and witnessed electronically. Banking and finance transactions can be governed by a mosaic of federal, state and territory laws, which would need to be amended to enable a seamlessly digital, paperless experience for the customer.

Recommendation 7: In considering how write access may be introduced the Inquiry should closely example and provide direction for:

(a) The development of a definition of write access. This will also ensure consistent language, noting the language differences in the Issues paper between opening an 'account' and managing a 'product'.

(b) Legal responsibilities of data holders and third parties (data recipients) in respect to transactions and data created and transferred through a write access process

(c) Scoping the relevant APRA and ASIC instruments, and the relevant AUSTRAC obligations under AML/CTF legislation to determine which aspects of these requirements can no longer be actively managed by the banks under write access and to determine an appropriate process for the updating of the relevant instruments and legislation

(d) A payments initiation feature within the CDR must be based upon and subject to the existing governance processes of the chosen payments scheme(s). The ABA does not support the establishment of a new payments mechanism for the CDR

(e) To consider other functions and features that may support a safe execution of write access including: digital Identity, electronic contracts and mortgages

(f) Consumer consent processes and consumer recourse to data recipients.

7. Linkages and interoperability with existing frameworks

The ABA supports the Issues paper position that the CDR should 'build upon and complement the arrangements businesses use, and not to displace them when they are used for future data-driven services.'[12]

It is the ABA's view that all regulatory frameworks and requirements must be reflected accurately to achieve the intended outcomes of those requirements in the CDR. The CDR should not displace existing frameworks which are fit-for-purpose and provide adequate governance oversight and consumer protections. The CDR should incorporate existing frameworks. Where those frameworks cannot operate efficiently in the data economy of the CDR, the regulatory and governance processes of those frameworks should be invited to update those instruments so that they can operate across the span of the real and data economy.

In the development of Open Banking, certain frameworks which are specific to banking have not been fully integrated into the design for launch. This is complex and technical work requiring a consideration

[12] Issues paper 2020 p6

of how instruments which operate in the real and digital economy can operate in the data economy. For example, complaints management and the banks' obligations under ASIC's Regulatory Guide 165 has only recently been considered in the context of Open Banking. Specific regulatory requirements which need to be considered include those issued by the regulators, ASIC and APRA. Additionally, banks obligations under AML/CTF legislation need to be built into the design of Open Banking.

Where Open Banking (and broader the CDR) design leads to a shifting of the banking functions to data recipients, the obligations on banks and data recipients under RBA, ASIC, APRA and AML/CTF requirements must be considered by those regulators. It is not equitable for banks to carry the burden of activities undertaken by unregulated third parties.

A review of the regulator instruments should consider whether:

- there is an additional or changed risk introduced by the design of Open Banking which can lead to:
    - In the case of an acceptable risk: An amendment to the instrument to account for the additional or changed risk introduced by the data recipient, and may place obligations on the data recipient or
    - In the case of an unacceptable risk: To reject the proposed CDR design until such a time that appropriate risk management processes can be developed.
- there is no additional or change risk introduced by the proposal in which case the existing instruments will continue to prevail.

Recommendation 8: In extending the CDR, a detailed consideration of the role of banking regulators (RBA, ASIC, APRA, AUSTRAC) and others such as payments governing bodies, and complaints management bodies should be undertaken to ensure a continuation of those governance arrangements under the CDR. The CDR should not be developing new banking governance structures where they already exist.

8. Consumer protection

Vulnerable Customers

The Open Banking development has predominantly focussed on consumer protections in the areas of privacy and data security. The Rules provide data holders with the ability to refuse to disclose where they consider it necessary to prevent physical or financial harm or abuse. Additional consideration will be required for customers experiencing vulnerability under write access.

Servicing the banking needs of customers experiencing vulnerability is a current consideration of the industry. ABA Banking Code of Practice 2020 (the Code) paragraph 38 describes customers who are experiencing vulnerability to include:

- age-related impairment
- cognitive impairment
- elder abuse
- family or domestic violence
- financial abuse
- mental illness
- serious illness or
- any other personal, or financial, circumstance causing significant detriment

A soon to be finalised ABA Guidance Paper for its members will provide further information to the banking industry which will assist in implementing consistent arrangements for customers who are

experiencing vulnerability. Open Banking Rules may challenge the ability of banks to fulfil these contractual obligations under write access. Any extension of Open Banking should also take the Code into consideration.

Customer data literacy

As Deloitte noted in their report[13], if consumers are going to take advantage of the benefits of Open Banking, and open data when the CDR is applied to other sectors of the economy, or make informed choices about banking products, they will need to understand the differences in financial value between different offers – they will need to be financially literate, financially capable, and financially conscious.

Therefore, in respect to consent, the education of consumers is even more critical. Customers need to be aware at every point that their data is being transferred from one party to another. In most use cases customers are not 'writing' data directly, they would be using a service from the provider, where the creation of data is a by-product (e.g. a service to make a payment or becoming a customer of a new institution). It is important that in seeking to make switching or other services more accessible for customers, data theft does not inadvertently become more prevalent.

Therefore, the introduction of the data economy through the CDR will create a new cohort of consumers in situations of vulnerability. Data literacy challenges will be added to existing financial literacy and digital literacy challenges. Whilst it may be that data literacy can assist in overcoming the other challenges, much of this will be determined by the extent and quality of data education available to the consumer.

The government has a lead role in the education of the public and vulnerable customers of the benefits of data literacy. CDR participants have a supporting role in helping to build the awareness and understanding of the CDR through their interactions with customers.

Recommendation 9: In respect to consumer protections

(a) Consideration should be given to consumer protections, and whether these should be ecosystem-wide protections, overseen by the CDR governing body to prevent offerings that would exploit vulnerable customers.

(b) The government has a role to play in leading education campaigns to raise data literacy/CDR understanding across all consumers and also to focussing on vulnerable cohorts.

(c) There should be incentives to encourage the development of propositions that benefit vulnerable consumers and provide compelling use cases to manage their financial data and protect their financial wellbeing.

9. Competition

The ABA supports reciprocal obligations. One of the strongest arguments for reciprocity is that it would deliver the greatest consumer benefit and is a core principle of data portability. However, the concept of reciprocity has narrowed over the course of developing Open Banking and this has repercussions for the way in which competition can be encouraged by the CDR.

Conceptually, reciprocity requires that subject to customer consent, the data recipient will be required to make available its 'equivalent data' to the ecosystem. That is, once an entity enters the CDR, its data is also designated. In this context, 'equivalent data' means customer data which is germane to the operations of the entity. For example, if a data recipient which is a telecommunications company accesses the credit card transaction history of a customer (with consent), the equivalent data which the

[13] Deloitte 2019, 'Open Banking: switch or stick' https://financialcapability.gov.au/files/open-banking-switch-or-stick-insights-into-customer-switching-behaviour-and-trust.pdf p44

telecommunications company would be designated to contribute to the CDR ecosystem might be customer mobile phone usage patterns (with consent).

However, the concept of 'equivalent data' has come to be narrowly interpreted as the 'same type of data'. Practically, this means that if a data recipient accesses banking data (with consent) is only obligated to supply banking data (with consent). If a data recipient does not hold banking data, it is not obligated to contribute data to the ecosystem.

This narrow interpretation of reciprocity has been adopted because of the siloed approach of sectoral designation to the CDR. Therefore, the designation sequence means that the CDR is being developed without best promoting competition and not necessarily as facilitative of innovation as it might otherwise be. Data holders are disadvantaged and the earlier a data holder is designated into the CDR the greater the competitive disadvantage

Therefore, reciprocity goes to the core of competition. Legal advice received by the ABA in June 2019 noted the inherent anti-competitive bias in the current designation process of the CDR:

> A lack of reciprocity is ultimately a detriment to consumer choice and creates an environment where competitive constraints are placed unequally on providers competing in the same data economy. A lack of reciprocity reduces the ability of all providers to harness the same data sets and compete, via their insights and analytics to make innovative products and services, thereby maximising benefits to consumers. For example, under the current proposal, a provider of a mobile wallet app, that is not a bank and does not participate in the services outlined in the designation instrument, would be able to obtain access to consumer data (with consumer consent), but the reverse would not apply: under the Draft Rules, a prospective competitor, such as a fintech, would not be able to seek mobile wallet data from the mobile wallet owner. This would leave the mobile wallet app provider with a significant advantage, as it would be the only company which could leverage both the mobile wallet data and all the other financial data designated under the designation instrument.'[14]

The legal advice recommended:

> Accreditation criteria that include, at a minimum, an obligation for data recipients to share any customer data they propose to combine with CDR data (Essential Data) obtained under the CDR in order to develop a product or service, where the customer has consented to that data being shared;
>
> To mitigate any risk that the reciprocity obligation would be a barrier to entry, an exemption to the obligations of reciprocity for small business and start-ups that meet each of the following: (a) have an annual turnover of less than $10 million in the most recent previous financial year; and (b) have fewer than 100 full-time equivalent (FTE) employees; and (c) have less than $3 million total debt to all credit providers, on a groupwide basis.'[15]

The ABA has previously noted the potential for data-rich companies to use the unequal playing field of the CDR. The ABA submission to the Digital Platforms Inquiry made the following point:

> 'The ABA notes that the ACCC will revisit the question of designation of the digital platforms into the Consumer Data Right (CDR). The ABA agrees that 'digital platforms may deliver significant benefits to current and potential future markets including through innovation and the development of new services' (p70). The ABA strongly encourages Treasury and the ACCC to consider prioritising the building out the CDR ecosystem. A CDR which is data rich will have positive network effects and be a regime which will fully be capable of delivering economy-wide innovation. As a principle, considerations for the

[14] Elizabeth Avery & Tim Kelly, G+T, 6 June 2019
[15] Elizabeth Avery & Tim Kelly, G+T, 6 June 2019

> designation of future sectors to the CDR should also look beyond a cost-benefit consideration (which is substantially grounded in the 'known present') and could also include an assessment on the potential of the data to contribute to future competition and innovation in the Australian economy.'[16]

In its final report of the Digital Platforms Inquiry the ACCC recognised:

> 'aside from addressing issues of market power, portability of data held by digital platforms may deliver significant benefits to current and potential future markets including through innovation and the development of new services. The ACCC will consider the benefits associated with digital platform data portability in the ordinary course as it considers sectors to which the Consumer Data Right regime may apply in the future.'[17]

The ABA urges the Inquiry to expedite considerations noted by the ACCC in its final report of the Digital Platforms Inquiry to 'revisit the applicability of the Consumer Data Right to digital platforms' and to implement reciprocity more broadly.

Reciprocity in its fullest sense, if not addressed, will have far greater consequences for the inherent competitive bias of the CDR.

Recommendation 10: All participants who are prepared to use consumer data via the CDR regime should be required to reciprocate, irrespective of whether those entities are within a designated sector. The principle of reciprocity will ensure all participants are incentivised to deliver the right outcome for consumers.

10. Leveraging Consumer Data Right infrastructure

CDR Governance

The current distributed governance structure of the CDR is not necessarily fit for purpose as the CDR evolves. The ACCC is the lead regulator which is responsible for the development of the Rules, accreditation process and the register. The Data Standards Body is responsible for standards development. The Office of the Australian Information Commissioner (OAIC) is responsible for oversight of the privacy standards. There is an outstanding question in respect to which entity is responsible for the security of the end-to-end ecosystem. There is no one entity ultimately responsible for the CDR.

Additionally, the Open Banking development has at times lacked a defined program management methodology. For example, there is no specific workstream which is managing the on-boarding of the non-major banks into Open Banking which is currently mandated for 1 February 2021. The CDR requires a strong and extensive programme management skill set with appropriate overall authority for the CDR and strong project management governance infrastructure.

The ABA notes the UK Open Banking system was developed by the industry using commercial principles (as opposed to legal Rules based principles) and a strong project management discipline. Additionally, the entirety of the Open Banking governance structure is contained to a single responsible entity.

[16] ABA Submission to the Treasury consultation on the Digital Platforms September 2019
[17] ACCC, Digital Platforms Inquiry, Final Report, June 2019, p30

Recommendation 11: This review to consider current governance arrangements of the CDR to create a stand-alone semi-government body which is:

(a) A single point of accountability.

(b) An entity that has human resources and funding capability to deliver such a significant economy-wide IT infrastructure project.

(c) An entity that can manage the complexity of such a build to ensure greatest possible commercial viability of that infrastructure. Including the undertaking of an extensive education programme for Australian consumers.

(d) Responsible for the end to end security of the ecosystem.

Data security in the digital economy

There are multiple aspects to security within the CDR.

Data recipients of banking data The ABA refers to comments in section 5 of this submission in respect to the importance of a tiered accreditation structure for data recipients which is commensurate to the type of data and the risks associated with the use cases proposed. Data security should not be diminished as data moves from banking to a different context.

Third party providers: In its submission to the ACCC Consultation on Third Party Providers (TPP) in February 2020 the ABA put forward principles for the development of rules for TPP in the CDR framework. These were:

1. Consumer consent – data management should not take place without meaningful and informed consumer consent
2. CDR data to be contented within the CDR ecosystem
3. Uniform security and privacy standards
4. TPPs to be accredited
5. Clear accountability and liability for resolving consumer complaints
6. Clear distinction between data recipients and TPPs roles
7. Clear delineation between CDR data and non-CDR data

The ABA would be pleased to provide the Inquiry with a copy of the submission.

Cyber-security capability: COVID-19 has demonstrated the significant detrimental impact of cyber-attacks on consumers and business. Currently there is no one entity which is responsible for the end to end security of the CDR. A cyber-security capability which is tasked with proactively identifying security risks to the CDR should be considered by the Inquiry. This capability should be responsible for coordinating and managing responses to cyber-security incidents/data breaches, cyber-security intelligence gathering including intelligence sharing and collaboration with accredited data recipients and data holders.

Recommendation 12: The establishment of a centralised CDR cyber-security capability, within the CDR governing body, which is separate to the internal security capabilities of the CDR. The centralised capability would be involved in intelligence gathering and coordinating responses to incidents and data breaches.

Privacy Safeguards

The ABA notes the robust privacy framework of the CDR. The Privacy Safeguards, bespoke to the CDR, are core to confidence and trust building. Given that the Privacy Safeguards will operate in addition to the Australian Privacy Principles (APPs) there is potential for confusion in respect to the context under which each framework is to apply. In its submission to the Treasury consultation on Open Banking Privacy Impact Assessment (PIA) in October 2019, the ABA made the following point:

> 'Generally, the operation of two privacy regimes creates complexity and the potential for confusion for both organisations subject to the APPs and Privacy Safeguards (PS), as well as for consumers in understanding their rights and protections. Clear guidance must be provided to ensure that the right consumer outcomes are achieved.'[18]

Consumers need to know their rights and protections to give their trust to the CDR and to participate with confidence that their data is subject to robust security and privacy requirements.

Recommendation 13: A comprehensive consumer government education programme to be undertaken in respect to consumer privacy rights under both the CDR Privacy Safeguards and the Australian Privacy Principles as a mechanism for engendering consumer confidence and trust in the CDR.

[18] ABA, October 2019, Submission to the Treasury consultation on Open Banking Privacy Impact Assessment (PIA)