Contact officer: Lisa Anne Ayres

23 Marcus Clarke Street
Canberra ACT 2601

GPO Box 3131
Canberra ACT 2601

www.accc.gov.au

12 December 2020

Senator Andrew Bragg
Department of the Senate
Chair, Select Committee on Financial Technology and Regulatory Technology

By email: FinTech.Sen@aph.gov.au

Dear Senator Bragg

ACCC supplementary submission to the Committee's Second Issues Paper

Please find attached the Australian Competition and Consumer Commission's (ACCC) submission responding to the second issues paper of the Senate Select Committee on Financial Technology and Regulatory Technology.

Should you have any queries about the issues raised in the submission, please contact Lisa Anne Ayres, General Manager Executive and Governance

Yours sincerely

Rod Sims
Chair

1. Introduction

The Australian Competition and Consumer Commission (ACCC) welcomes the opportunity to respond to the Second Issues Paper of the Senate Select Committee on Financial Technology and Regulatory Technology (Senate Committee).

The ACCC promotes competition and fair trading in markets to benefit consumers, and the Australian community. We do this primarily through administering the *Competition and Consumer Act 2010* (Cth) (CCA). We are the lead implementation agency for the Consumer Data Right, which was established under Part IVD of the CCA.

The Consumer Data Right (CDR) is being implemented according to four key principles that it should be:

1. **consumer focussed** - it should be for the consumer, be about the consumer and be seen from the consumer's perspective.
2. **encourage competition** - it should seek to increase competition for products and services available to consumers so that consumers can make better choices.
3. **create opportunities** - it should provide a framework from which new ideas and business can emerge and grow, establishing a vibrant and creative data sector that supports better services enhanced by personalised data.
4. **efficient and fair** - it should be implemented with security and privacy in mind, so that it is sustainable and fair, without being more complex or costly than needed.

This submission provides an update to the Senate Committee on the progress of implementing the Consumer Data Right. We also address a number of issues raised by the Senate Committee, which are relevant to the ACCC's remit as prescribed by the CCA and experience in implementing the Consumer Data Right.

2. Banking sector implementation

Implementation of the Consumer Data Right in banking is steadily progressing, with a number of milestones now complete. Despite challenges from COVID-19, throughout 2020 we continued to deliver on time and within budget to a schedule agreed in December 2019.

The milestones achieved together with upcoming milestones are summarised below:

- February 2019: Major banks' product reference data (PRD) obligations commenced
- May 2020: Register and Accreditation Application Platform (RAAP) released
- July 2020: Major banks commenced live data sharing of Phase 1 consumer data (personal accounts including savings and term deposits)
- September/October 2020: Conformance Test Suite (CTS) launched to enable accredited data recipients (ADRs) and data holders to test their conformance with the Consumer Data Standards and Consumer Data Right Register design. The CTS was expanded in November to facilitate testing for commencement of Phase 2 functionality
- October 2020: Non-major authorised deposit-taking institutions (ADIs) PRD obligations commenced
- October 2020: New rules commenced to permit the use of accredited intermediaries to collect consumer data

- November 2020: Major banks commenced sharing of Phase 2 datasets and functionality (home loans and personal loans, joint accounts, closed accounts, direct debits, scheduled payments and payees)
- As of 9 December 2020:
    - There are five data holders and six ADRs, with a further four data holders in the process of on-boarding to the Register.
    - We have granted access to the CDR Participant Portal to over 130 entities, which allows them to draft and submit applications to become accredited.
    - 51 potential data recipients have begun drafting accreditation applications.
    - The ACCC recently updated its education and guidance to help businesses complete their accreditation applications.
    - According to a recent survey by Frollo and NextGen.Net, 71% of industry respondents indicated that they intend to use the Consumer Data Right, with 58% of these stating that they intend to use CDR data within the next 12 months.[1]

In terms of next steps, in February 2021 major banks are scheduled to commence sharing of Phase 3 consumer data (business finance, investment loans, lines of credit, overdrafts, asset finance, cash or farm management accounts, pensioner deeming accounts, retirement savings accounts, trust accounts, foreign currency accounts, consumer leases).

3. Energy sector preparations for implementation

The Senate Committee requested an update on the progress of preparatory work for the rollout of the Consumer Data Right in the energy sector.

Work is progressing on the implementation of the Consumer Data Right in the energy sector. Significant milestones completed include:

- February 2019: Public consultation on data access models for energy data.
- August 2019: Publication of position paper proposing gateway data access model for energy data.
- June 2020: Designation by the Treasurer of the energy sector and specific data sets to be subject to the Consumer Data Right.
- July 2020: Public consultation on energy rules framework.

We continue to work to the following:

- February 2021: Expected consultation of draft rule amendments required for implementation of the Consumer Data Right in the energy sector to commence.
- June 2021: CDR Rules for the energy sector are expected to be made.
- Subject to future design and funding considerations, product data sharing is expected to commence in the first half of 2022 and consumer data sharing is expected to commence between late 2022 and early 2023.

[1] Frollo and NextGen.Net, *The State of Open Banking in Australia*, November 2020, https://frollo.com.au/open-banking/state-of-open-banking-report-2020/, pp.13 and 17, viewed 5 November 2020. The survey consisted of 161 respondents including brokers (28%) and aggregators (8%), banks and lenders (22%), fintechs (20%), technology providers (11%) and others (11%) including consultancies.

The Consumer Data Right in the energy sector differs in how it was implemented in banking in two key ways:

- it relies on a gateway access model (Australian Energy Market Operator), and
- designated consumer data sets are distributed across multiple data holders.

Changes to the national energy laws are required to facilitate implementation of the Consumer Data Right in the energy sector. The Commonwealth Department of Industry, Science, Energy and Resources is leading this work in coordinating with relevant State and Territory agencies. Ministerial agreement is expected be obtained during 2021.

4. Big bank acquisitions of fintechs

We note the Senate Committee's interest in the role of Australia's merger laws with regard to the acquisition of fintechs by big banks.

Australia's merger law under the CCA seek to ensure that changes in market structures, through businesses acquiring other businesses do not harm competition. Section 50 of the CCA prohibits acquisitions of shares or assets that would have the effect, or be likely to have the effect, of substantially lessening competition in any market in Australia.

The ACCC also has a mandate to analyse and report to government in relation to competition issues that arise in financial services markets through a series of market studies and inquiries at the direction of the Treasurer.

The Australian banking sector is dominated by the presence of four major banks which hold substantial market power as a result of their size, strong brands and broad geographical reach. The emergence of fintechs into the Australian banking sector has brought with it new innovative technology and systems which have the potential to challenge the established financial institutions and facilitate faster, cheaper and more efficient services for consumers.

These small firms, including some start-up firms, can drive significant aspects of competition, such as pricing, innovation or product development, even though their own market share may be small. Acquisitions of these vigorous and effective competitors by large rivals may remove an important driver of competition in the market.

In some markets where rivalry between the incumbents is limited, the major constraints may come from potential or emerging competition. Firms with substantial positions in these markets can undermine this process by acquiring emerging competitors before they have the opportunity to potentially become a substantial threat.

Acquisitions by the big four banks of small but vigorous and effective competitors in the market has the potential to substantially lessen competition and therefore the ACCC will carefully scrutinise such transactions. This does not mean however that all acquisitions of fintechs by the big four banks will necessarily raise competition concerns. It will depend on the circumstances of each case, including assessing the barriers to entry for new competitors to emerge.

While it is recognised that fintechs require significant capital investment to expand to the level where they can compete outside niche sectors of the market, it would be concerning from a competition perspective if this capital investment were to only arise through acquisitions by the four incumbent major banks.

5. Consumer Data Right and 'Big Tech' companies

Given the potential for big non-bank technology companies such as digital platforms ('Big Tech' companies) to participate in the Consumer Data Right, the Senate Committee expressed interest in the kinds of measures that may be required as the Consumer Data Right evolves to ensure it increases competitive forces in Australia.

Big Tech companies can become CDR participants compulsorily by Government designation or voluntarily by applying for accreditation.

5.1. Designation of Big Tech

The Government designates sectors and specific data sets within each sector to which the Consumer Data Right will be applied.

Following a sectoral assessment, it is open to the Government to specify in a designation instrument:

- classes of information (datasets) held by Big Tech companies, and
- Big Tech companies as data holders.[2]

The sectoral assessment could be specific to Big Tech, or could relate to a sector in which Big Tech companies participate.

The following is a hypothetical example to demonstrate how this may operate. The Government designates location data as a class of information relevant to designation of the taxi and ride share sector. The Government also specifies Google as a data holder, bringing within scope consumer data collected through Google Maps.

In this scenario, Google would be required to share relevant consumer data with ADRs at the direction of the consumer. A consumer may direct their location data to be shared with their accredited bank when travelling overseas to avoid the effort involved providing their travel details to their bank ahead of time. A more sophisticated service offering could be automated currency conversion or selection at the point of sale.

As part of its Digital Platforms Inquiry (DP Inquiry), the ACCC analysed ways portability and interoperability could promote competition between digital platforms. This analysis included consideration of applying the Consumer Data Right to digital platforms to promote competition in existing markets and assist competitive innovation in future markets.[3]

The DP Inquiry did not consider competition and consumer issues arising from the entry of a Big Tech firm into banking and financial services.

The ACCC chose not to recommend increased data portability obligations to address the market power and competition issues, because, specific to the markets the DP Inquiry examined, such obligations were unlikely to significantly address these issues in the short term. It did, however observe that there were other benefits associated with data portability and sharing (such as the development of new products and innovative offerings) that should be considered in the course of determining which sectors the CDR regime would apply to in future.[4]

---

[2] Section 56AC(2), CCA

[3] ACCC, *Digital Platforms Inquiry Final Report*, 26 July 2019, https://www.accc.gov.au/system/files/Digital platforms inquiry - final report.pdf, p.11

[4] ibid, , pp.11, 115-116

Designating digital platforms as a sector will raise a number of complexities, due to the breadth and integration of Big Tech firms across the economy. This approach could have unintended consequences and requires in-depth analysis. As noted in the DP Inquiry's final report, the Consumer Data Right is just one way to require digital platforms to share data with potential rivals. Another would be interoperability with other services. Before a solution is chosen, various factors need to be taken into account including the extent to which network effects in these markets might restrict the incentives for portability, privacy concerns, and identifying the extent and nature of data to be shared.[5]

5.2. Big Tech and Accreditation

The ACCC understands the Senate Committee is interested in whether the regulatory framework governing use of financial data is adequate for promoting competition, including in circumstances where a Big Tech company applies to be an accredited data recipient in order to provide services to consumers.

The accreditation regime is intended to promote consumer trust in the Consumer Data Right ecosystem, and represents a small component of the regulatory framework governing financial data.

The ACCC draws on a range of tools to respond to competition issues. These tools do not form part of the CDR accreditation framework. However, in certain circumstances, competition matters may be considered relevant to the assessment of whether an accreditation applicant is a fit and proper person to manage CDR data.

5.2.1. Accreditation criteria

The ACCC assesses accreditation applications on a case by case basis, within the framework prescribed by the relevant legislation and rules.

Currently under the legislative framework, any person in Australia or overseas who wishes to receive CDR data from a data holder to offer products or services to consumers must be accredited. Applicants must demonstrate that they have satisfied the criteria for accreditation under the CDR Rules, including:

- information security requirements to protect consumers' data from misuse or unauthorised access
- being a fit and proper person to manage CDR data
- appropriate dispute resolution processes, and
- adequate insurance.[6]

A foreign entity that wants to become accredited is required to have a local agent, and include details of its local agent and its local agent's address for service in its application for accreditation.[7]

Factors relevant to the assessment of the fit and proper person requirement include whether the applicant or any associated person/s has:[8]

- been convicted of a serious criminal offence or offence of dishonesty within the past 10 years in Australia or a foreign jurisdiction

[5] ibid, p.11

[6] Competition and Consumer (Consumer Data Right) Rules 2020 (CDR Rules), Rule 5.5

[7] CDR Rules, r 5.2

[8] CDR Rules, r 1.9

- been found to be in contravention of any law relevant to the management of CDR data in Australia or a similar law in another country
- been the subject of a privacy determination[9] in Australia or another country
- a director that has been disqualified from managing corporations or is subject to a banning order (if a body corporate)
- a history of insolvency or bankruptcy
- been subject to a determination under an external dispute resolution scheme recognised under the Privacy Act or a finding or determination under a similar law in another country that included a requirement to pay monetary compensation.

The ACCC can also take into account any other relevant matter, including but not limited to the objects of Part IVD of the CCA.

Broadly, the objects of Part IVD are to enable:

- consumers to request businesses to disclose the consumer's own data to an accredited person who can use that data to provide services to the consumer
- any person to efficiently and conveniently access product information

in order to create more choice and competition or otherwise promote the public interest.[10]

The information received and analysis undertaken when assessing an accreditation application is, in isolation, unlikely to provide a sufficient basis for forming a view on competition impacts arising from accreditation. Competition assessments generally involve market enquiries, information gathering and in-depth analysis. Compelling evidence from authoritative sources would be required for the ACCC to determine an accreditation applicant did not satisfy the fit and proper person requirement on account of matters relevant to the objects of Part IVD.

5.3. Obligations of Accredited Data Recipients

Accredited data recipients are subject to several continuing obligations. Obligations relevant to the issues raised by the Senate Committee include:

- compliance with relevant CDR Privacy Safeguards, and
- reciprocity.

Accredited persons may only collect and use CDR data with the consent of the consumer. The CDR Rules require that a consumer's consent be voluntary, express, informed, specific as to purpose, time limited and easily withdrawn.[11]

---

[9] A determination under paragraph 52(1)(b) or any of paragraphs 52(1A)(a), (b), (c) or (d) of the *Privacy Act 1988*

[10] Specifically, section 56AA of the CCA provides:

> The object of this Part is:
>
> (a) to enable consumers in certain sectors of the Australian economy to require information relating to themselves in those sectors to be disclosed safely, efficiently and conveniently:
>
> i. to themselves for use as they see fit; or
>
> ii. to accredited persons for use subject to privacy safeguards; and
>
> (b) to enable any person to efficiently and conveniently access information in those sectors that:
>
> i. is about goods (such as products) or services; and
>
> ii. does not relate to any identifiable, or reasonably identifiable, consumers; and
>
> (c) as a result of paragraphs (a) and (b), to create more choice and competition, or to otherwise promote the public interest.

[11] CDR Rules, r 4.11 and r 4.13

In seeking consent from a consumer, ADRs must also comply with the Consumer Experience standards and have regard to the Consumer Experience Guidelines when developing their consent processes.[12]

5.3.1. Privacy Safeguards

The CDR Privacy Safeguards in the CCA[13] provide additional protection for CDR consumers by governing how their CDR data must be treated by data holders and ADRs. The ACCC and the Office of the Australian Information Commissioner (OAIC) are co-regulators of the Consumer data Right, with the OAIC having a primary role for the enforcement of the Privacy Safeguards and rules relating to privacy and confidentiality.

Collection of CDR data is limited by the data minimisation principle, which provides that an accredited person:

- must not collect more data than is reasonably needed in order to provide the requested goods or services, including over a longer time period than is reasonably required, and
- may use the collected data only in accordance with the consent provided, and only as reasonably needed in order to provide the requested goods or services.[14]

Privacy Safeguard 6, together with CDR Rules 7.5 and 7.7, set out key obligations and restrictions on ADRs in the use and disclosure of CDR data.

An ADR may only use a consumer's CDR data in accordance with express, informed and current consent from the consumer. ADRs must obtain consent from CDR consumers of the CDR data they collect and notify consumers when they have collected such CDR data.

The term 'use' includes:[15]

- the entity accessing and reading the CDR data
- the entity making a decision based on the CDR data
- the entity de-identifying the CDR data,[16] and
- the entity passing the CDR data from one part of the entity to another.

The consent requirements in the CDR Rules are stronger than those which currently apply to Big Techs under the *Privacy Act 1988* (Cth). ADRs must implement relevant security controls as set out in the CDR Rules to remain compliant with the CDR Privacy Safeguards. CDR Privacy Safeguard 12 mandates that ADRs protect CDR data from misuse and unauthorised access or disclosure and delete or de-identify redundant data in accordance with the CDR Rules.

[12] CDR Rules, r 4.10

[13] Part 1VD, Division 5, CCA

[14] CDR Rules, r 1.8

[15] OAIC, *CDR Privacy Safeguard Guidelines*, version 1.0, https://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines/chapter-6-privacy-safeguard-6-use-or-disclosure-of-cdr-data-by-accredited-data-recipients-or-designated-gateways/, Chapter 6, paragraph 6.11

[16] CDR Rules, r 7.5 (1)

5.3.2. Reciprocity

Under the CCA and CDR Rules, reciprocity applies in respect of CDR data that is:

- generated and held by or on behalf of an accredited person, and
- generated in respect of a product that is publicly offered by the accredited person to consumers and relates to data specified by a designation instrument.[17]

Reciprocity does not apply to materially enhanced information.[18]

Reciprocity is intended to apply across sectors, with data sharing required between sectors which have been designated. This means that entities from a sector other than banking will be able to become ADRs and may receive data, but reciprocal data rights will only apply to the extent the ADR already holds designated data or becomes subject to a future sector designation instrument.

For example, under the CDR rules a non-ADI lender that is accredited will become a reciprocal data holder in respect of data they generate for their personal loan products. A non-ADI accredited person that provides a budgeting app, but does not offer any of the banking-like products specified in a designation instrument, will not be a reciprocal data holder.

6. Potential for CDR to interact with other jurisdictions

We note the Senate Committee's interest in the potential for Australia's CDR to interact with open banking data sharing schemes in other jurisdictions.

We support mutual recognition of accreditation with other jurisdictions, and work with relevant agencies responsible for progressing the overarching policy frameworks that would facilitate these outcomes.

Where appropriate, we seek to leverage existing standards to reduce the potential costs for participants. For example, we recently announced our intention to recognise particular existing standards as evidence of meeting the information security requirements under the CDR Rules. These included:

- partial recognition of ISO 2700, for the purposes of accreditation at the restricted level. ISO 2700 is an international standard on how to manage information security
- recognition of persons meeting ATO's Digital Service Provider (DSP) Operational Framework (OPF) requirements to its highest 'standard' for a particular software product. This applies where a DSP has a product or service with more than 10,000 taxpayer or superannuation records.

Globally, there are diverging approaches to data sharing regimes in various stages of development and implementation. Whereas the Consumer Data Right prescribes data standards and mandates participation on market participants operating within designated sectors, some other regimes are limited to portability requirements without prescribing the form in which data must be shared.

[17] Section 56AJ of the CCA sets out the meaning of data holders, which includes accredited persons holding information specified in a designation instrument. Schedule 3 of the CDR Rules specifies when reciprocal data holder obligations commence for the banking sector.

[18] Section 10, Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019, 4 September 2019

Different approaches have been adopted based on the respective policy intent of each jurisdiction. These differences will impact the extent to which interaction, in the sense of interoperability, between different schemes is possible. The Data Standards Body supports the principle of interoperability, and the use of open, robust and widely used standards wherever possible.[19]

While facilitating interaction between the Consumer Data Right and relevant schemes being implemented in other jurisdictions may generate certain benefits for Australian consumers, including the potential for increased competition, these outcomes are not guaranteed. Overseas requirements may not be suitable for Australian consumers or industry. As a preliminary step, careful analysis of the potential risks and benefits should be undertaken, with particular reference to the policy objectives of relevant schemes to mitigate against unintended consequences.

[19] Data Standards Body, Consumer Data Standards, v 1.5.1, https://consumerdatastandardsaustralia.github.io/standards/#standards,Outcome principle 2: APIs use open standards