12 September 2018

Daniel McAuliffe
Structural Reform Group
The Treasury
Langton Crescent
PARKES ACT 2600

Via Email: data@treasury.gov.au

The Commonwealth Bank welcomes the opportunity to respond to the exposure draft of the Consumer Data Right legislation.

As one of the first organisations to be delivering the Consumer Data Right, the Commonwealth Bank is enthusiastic about its potential economic benefits for Australian consumers and businesses. For consumers, data-driven innovation will deliver new services, increase transparency and provide more choice among financial products.

For the Commonwealth Bank, it will provide an opportunity to improve the financial wellbeing of the customers and communities we serve. It will, for instance, provide a way for our customers to share a holistic snapshot of their finances in a safe and secure manner. A regime of mutual-data sharing based on reciprocity will deliver greater benefits to consumers by encouraging investment and enabling data-driven innovation.

It is important to build consumer trust and confidence in the Consumer Data Right from the beginning. This will only occur if consumers can trust that their data is protected by appropriately robust security practices; can be assured that in sharing data they are not undermining their privacy; and that they are able to provide consent, in a meaningful and informed manner, for the purpose and period their data is being used.

For the CDR to achieve its objectives for customers and the economy, the sharing of data must be in line with identified public policy goals, with clearly defined parameters regarding the types of data that will be shared. In this context, the Commonwealth Bank believes the scope of datasets in the Bill is too broad and reflects a departure from the findings of the two expert reports to Government on the regime. A requirement to share value added data that is too broad would significantly undermine incentives for investment in customer-facing innovations, from both small and large innovators.

The Commonwealth Bank views that the timelines to deliver the first tranche of the Consumer Data Right are ambitious but achievable – and most importantly, can be met without sacrificing any of these important consumer safeguards on the current proposed roadmap for the legislation and rules.

Contents

Summary of Recommendations

Recommendation 1
The Minister should only be empowered to designate datasets which have the following characteristics:

- the datasets must be about the products and services supplied by the class of persons designated as data holders for the relevant sector;
- the datasets must be about CDR consumers;
- the datasets must be collected and held by or on behalf of the data holder in digital form; and
- the data must have been generated or collected from the date of commencement of the CDR regime for a designated sector.

Recommendation 2
A new, more precise, definition of CDR data should be developed by reference to principles including:

- CDR data should only include raw data and information computed from such raw data if that information: is required to make that raw data intelligible; does not result from a process of material enhancement; and will not reveal commercially confidential information (including trade secrets) of a data holder if disclosed to a third party.
- 'Value added data' should be excluded from the CDR regime.

The legislation should ensure that the ACCC be required to conduct a cost-benefit analysis where new CDR data datasets are included in the CDR regime. The legislation should also allow prices to be set in the ordinary operation of the market for the provision of this derived data.

Recommendation 3
Amend the definitions of CDR data and CDR consumer so that the CDR regime applies to information about a person who acquires, or has acquired, goods or services from a data holder.

Recommendation 4
The Bill should provide a minimum public consultation period to provide stakeholders of potential designated sectors with the time to consider and respond to the proposed instrument of designation.

Recommendation 5
The Bill should provide for consultation regarding the designation of classes of datasets to comprise CDR data for a designated sector. Section 56AD should set out more comprehensive factors for consideration when designating data sets.

Recommendation 6
The ACCC should be bound by a set of principles or objectives determined by the Minister when making the Rules and should specifically be required to consult with relevant data holders with respect to any such rules. For the banking sector, such a determination should be made requiring the ACCC to implement the recommendations of the Review into Open Banking.

Any report the OAIC provides to the ACCC in considering the proposed Rules should be made publicly available.

Recommendation 7
The Bill should determine non-exhaustive baseline accreditation criteria (such as those set out in section 2.4) for the banking sector which should contain requirements to ensure recipients have

sufficient resources and processes and appropriate management as a prerequisite to being trusted with CDR data.

The Bill should distinguish between datasets that can be disclosed to non-accredited recipients and datasets that cannot. This could be dealt with by Ministerial determinations or other instruments issued on a sector by sector basis.

Recommendation 8
The Government should further consider the reciprocity principle outlined in the Review into Open Banking in order to encourage greater usage of the CDR regime for the benefit of consumers and to further encourage and stimulate innovation and competition across markets.

The Bill should reflect the principle that any accredited data recipient should be under an obligation to make data generated or held by that recipient from goods or services supplied to a CDR consumer available as CDR data to data holders and other accredited data recipients at the direction of a CDR consumer.

Recommendation 9
The Rules should include safeguards against the disclosure of CDR data to accredited data recipients in certain circumstances, rather than this being a provision which the ACCC may optionally include in the Rules. These safeguards could include exemptions from disclosure of CDR data by data holders:

- to accredited data recipients that no longer meet the accreditation criteria (including not maintaining appropriate security standards), whose accreditation has been suspended or varied or revoked, or where the data holder reasonably suspects it has suffered an unauthorised disclosure of CDR data; and
- in emergency circumstances, such as a security breach of one or more CDR participants that is substantially affecting the operation of CDR regime for the banking sector. These exemptions are necessary for the protecting security of CDR data for CDR consumers and to preserve the integrity of the CDR regime.

Further, the Bill should include provisions for data holders to withhold the supply of data to accredited data recipients who have not taken 'reasonable steps' to secure their customer's data or CDR data.

Recommendation 10
Sector regulation, mandatory Prudential Standards and generally applicable industry standards should be consulted at all steps of the CDR process – from designation, to determining the Rules, to considering the application of protections such as the privacy safeguards.

To the extent of any conflict or inconsistency between such standards or regulation and any of the privacy safeguards, instrument of designation, Rules, and data standards, mandatory Prudential Standards or other sector regulation should take precedence.

Recommendation 11
The relationship between data holders and data recipients and their obligations should be clarified.

Limb (d) of the definition of accredited data recipient should be deleted to take into consideration that a person may be both a data holder and an accredited data recipient with respect to some datasets.

The obligations on data holders and data recipients in respect to protection of CDR data should be the same.

The Rules should provide for the modification of the accreditation regime for accredited data recipients so that there are appropriate exemptions from the accreditation requirement for related bodies corporate which share the same accredited IT systems with the accredited data recipient.

Recommendation 12
The meaning of what is generated or collected in Australia should be further clarified in the Bill.

Foreign corporations without an appropriate presence in Australia should not be permitted to be accredited data recipients.

The extraterritorial application of the Bill should align with the extraterritorial application of the Privacy Act, such that foreign entities which are CDR participants should be subject to the Privacy Act.

Recommendation 13
The Government should re-consider the purpose for introducing the Privacy Safeguards with a view to reducing the number of safeguards to only those permitting disclosure by a data holder to a data recipient and regulating collection, use and disclosure of CDR data by an accredited data recipient.

The Privacy Safeguards should not restrict or prevent any use of CDR data by the data holder which would otherwise be permitted based on it already being held.

Privacy Safeguard 6 should be modified so that it only applies to the actual disclosure by a data holder of CDR data in response to a request by the relevant CDR consumer.

Privacy Safeguard 7 should be modified to exclude the Spam Act from applying to authorise the use or disclosure of CDR data for direct marketing.

Privacy Safeguard 8 should be modified:

- so that CDR data can only be disclosed on the request of a CDR consumer to a foreign data recipient that is accredited under subsection 56CE(1) of the Bill and the conditions specified in the Rules are met (in other words, substitute 'or' after subsection 56EK(c) to 'and');
- to ensure that data holders and accredited data recipients are not restricted, or subject to conflicting obligations, with respect to using off-shore service providers as part of their information technology infrastructure; and
- to ensure that cross-border disclosure of CDR data to, and use by, suppliers for the provision of IT services or outsourcing arrangements within a data holder's or accredited data recipient's IT infrastructure are governed by the Privacy Act (regarding personal information) and the accreditation regime (regarding implementation of technical, organisational and contractual security measures).

Privacy Safeguard 10 should be amended to contain exceptions to inform CDR consumers that include:

- where CDR consumers have already been informed the CDR data was inaccurate, out-of-date or incomplete;
- where a third party will assume the obligation to inform the CDR consumer; or

- where the data holder, despite taking all reasonable steps to keep CDR data up to date, complete and accurate, does not have the current contact details of the relevant CDR consumer to inform them.

Recommendation 14

The Bill does not consider the interaction between the CDR and the separately proposed *National Consumer Credit Protection Amendment (Mandatory Comprehensive Credit Reporting) Bill 2018* (**CCR Bill**). If CDR consumers are authorised to direct the provision of any information related to them to an accredited data recipient (where the data holder is a credit provider) the CCR Bill may become redundant.

The disclosure of credit eligibility information and mandatory credit information should not be authorised by the CDR Bill or potentially authorised under the Rules on the basis that the Part IIIA of the Privacy Act and the CCR Bill are specifically designed to address credit eligibility information and mandatory credit information.

Recommendation 15

The ACCC should be limited to only recognise Australian external dispute resolution schemes when exercising its power under s56DA(1) of the Bill.

Recommendation 16

The enforcement of data standards against both data holders and accredited data recipients under the CDR regime be simplified by being undertaken by the ACCC. This would be effected by:

- removing the provisions deeming data standards as multi-lateral contracts; and
- introduction of a materiality threshold to trigger the right for aggrieved persons to bring enforcement proceedings for material breaches of the data standards.

The Bill should provide:

- for the civil penalty regime to be applied in respect of the proposed Part IVD of the CCA is the civil penalty regime contained in the Privacy Act; and
- the power for the ACCC to delegate functions and powers be removed.

The Bill should:

- provide for the liability shield to remain unaffected except if a person breaches Part IVD, the regulations made for the purpose of Part IVD, or the Rules, then that person would be liable for a breach of that specific provision; and
- be amended by removing the burden of proof requirement for those seeking to rely on the liability shield.

1. Scope of CDR Data

The Commonwealth Bank's view is that the Open Banking reforms will generate new opportunities for innovation beyond those transactions that will be captured by the Consumer Data Right framework.

The Commonwealth Bank currently has numerous data agreements with third parties. In the future the investment in technology, and the uplift in consumer education that will flow from it, will reduce the effort for customers to send their data between firms – even for data not specifically mandated in the Consumer Data Right.

It is possible for companies to monopolise raw inputs – in this case, the raw data – but it is not possible for one company to monopolise innovation. As such, the framework should focus on the raw data generated by consumers and any market interventions beyond this scope should carefully weigh any benefits against future costs.

1.1 What is CDR data?

The Bill defines CDR data as being data specified by the Minister in an instrument (as well as data derived from that data). Accordingly, any data could be designated and constitute CDR data.

The Open Banking reforms in the UK (the **UK regime**) sets out comprehensive objectives and considerations to which the Payment Services Regulator must have regard when discharging its functions.[1] It must, for instance, consult with the UK treasury about whether to make a designation order with respect to payment systems.[2] Other objectives and considerations include:[3]

- ensuring that systems are developed in a way which promotes the interests of consumers;
- promotion of innovation in the interests of consumers;
- the ease with which a participant can change its systems;
- the needs of participants that are operating systems;
- the costs associated with participation;
- the principle that a burden or restriction which is imposed on a person should be proportionate to the benefits;
- differences in the nature of, and objectives of, businesses carried on by participants; and
- the principle that the regulator should exercise its functions as transparently as possible.

Consideration should be given to the development of similarly directed objectives to apply to the Minister and, as noted in Recommendation 6, the ACCC.

Accordingly, the Commonwealth Bank recommends that the Bill set parameters within which the Minister must operate in determining the datasets to be designated as CDR data (see Recommendation 1).

---

[1] As set out in the Financial Services (Banking Reform) Act 2013 and Payment Services Regulation 2017 (2017 No. 752)

[2] Please see Part 5 of the UK *Financial Services (Banking Reform) Act 2013, in particular ss43 - s45, and s49.*

[3] Please see s124(2) and s106(3) of the *Payment Services Regulation 2017 (2017 No. 752) and ss40 – 55 of the Financial Services (Banking Reform) Act 2013.*

Recommendation 1
The Minister should only be empowered to designate datasets which have the following characteristics:

- the datasets must be about the products and services supplied by the class of persons designated as data holders for the relevant sector;
- the datasets must be about CDR consumers;
- the datasets must be collected and held by or on behalf of the data holder in digital form; and
- the datasets must have been generated or collected from the date of commencement of the CDR regime for a designated sector.

1.2 Inclusion of derived data

The Bill builds on the Productivity Commission's report on Data Availability and Use and the independent Review into Open Banking.[4] Those reviews recommended that a distinction be drawn between data generated directly from the activities of a customer (the 'raw data'), and the insights or analysis derived from that data (the 'value-added data').[5]

In contrast to those reviews, the Bill is framed broadly and captures not only raw data, but also information derived from that raw data (referred to as 'derived data'). The inclusion of derived data as CDR data significantly expands the scope of data potentially subject to the regime from 'raw' observable customer provided data, to 'value-added data' which could extend to any information held by a bank or other CDR holder.

The Commonwealth Bank understands that the inclusion of derived data may be seeking to address a limited number of use-cases. For example, the Productivity Commission listed specific use cases, such as wearable devices, where there is a customer benefit in sharing more than the raw data. [6] In its raw form certain data might not be meaningful to a consumer and requires some degree of transformation to be intelligible. The legislation may also be seeking to ensure that where a minor transformation of raw data (which requires little or no investment or effort), that data is included in the CDR regime.[7]

In each case listed above, there is no proprietary right or confidential information (such as a trade secrets) used to transform the raw data.

---

[4] Productivity Commission, 2017, 'Inquiry Report: Data Availability and Use', released 8 May; Recommendation 3.3. Farrell, S., 2017, 'Review Into Open Banking: Giving Customers Choice, Convenience and Confidence'.
[5] The PC recommended (at p.207): *'The basic principle would be that when multiple data sources are transformed to an extent that it is merely probable (but not certain) that a characteristic is associated with an individual consumer, then this data would most likely be proprietary information of the data holder'.* Recommendation 3.3 of the Review into Open Banking recommended that 'data that results from material enhancement by the application of insights, analysis or transformation by the data holder should not be included in the scope of Open Banking.'
[6] Productivity Commission, 2017, p.203. The Commission also listed 'Know Your Customer' assurances generated by banks, which would need significantly more investigation to understand the interaction with current legal requirements on banks.
[7] The Productivity Commission stated that it does 'not consider that data that has been cleansed of errors, made better through simple statistical means such as aggregated or averaged for each consumer but otherwise unaltered, or made machine readable could singly or collectively be construed to be value added (as some might argue)'. Productivity Commission, 2017, 'Inquiry Report: Data Availability and Use', released 8 May, p.201

1.2.1 Unintended consequences of vaguely defined parameters for designated data

The inclusion of a broad definition of CDR data will likely have unintended consequences for the designated sectors of the Australian economy. In particular, such an expansive definition of CDR data may result in value-added datasets which are related to designated data sets being subject to the CDR regime despite being commercially sensitive, proprietary or unique.

Derived data will often contain material enhancements and transformation which, if disclosed to a third party, can reveal commercially confidential information (including trade secrets) of data holders. Mandating such disclosures would have the likely consequence of reducing investment in market differentiation and could have a chilling effect on data-driven innovation by designated sectors of the economy. As a result, many of the potential benefits to consumers of the regime may not be realised.

In addition, the practical difficulties in making derived data available in the same manner as raw data (or minimally transformed data) would likely make sharing such data uneconomic. Data that results from the application of a process or the process of transformation are not typically standardised or comparable. The ability for consumers to compare and aggregate personal financial information across providers in the market requires a measure of standardisation. Arriving at a common point will require additional investment by participants to achieve this.

1.2.2 Fees

The Commonwealth Bank supports the principle that a fee may be charged for certain data, especially for derived data. However, the Commonwealth Bank believes that further consultation is required to determine the most appropriate mechanism for setting prices. As such, the principle should be retained in the Bill but the ACCC should not be given power to set fees for the transfer of derived data. In many cases, the market may achieve a more efficient outcome in valuing non-comparable, transformed and unique datasets.

The effects of mispricing of such data would be the massive transfer of value from businesses operating within the regime, undermining the efficient operation of the market. There may be some mechanisms the ACCC could use to monitor operation of the market and to prevent CDR participants from misusing their market power, such as penalties.

1.2.3 Recommended approach

The Commonwealth Bank supports the intent of the Bill to ensure consumers and businesses derive value from the information being shared by preventing minimally transformed data from falling outside the regime. However, a finer distinction can be made between 'derived data' generally and those exceptional use cases we understand that the Government seeks to solve for. To this end, the Commonwealth Bank proposes that a new, more precise definition of CDR data could provide greater certainty to businesses regarding the scope of the Consumer Data Right and the protection of investment and proprietary rights or other confidential information, while delivering real benefits to consumers.

The Commonwealth Bank has developed a set of preliminary principles which it considers could be applied to assist in developing a new more precise definition of CDR data (see Recommendation 2) and a proposed framework for implementing those principles (see Figure 1 below).

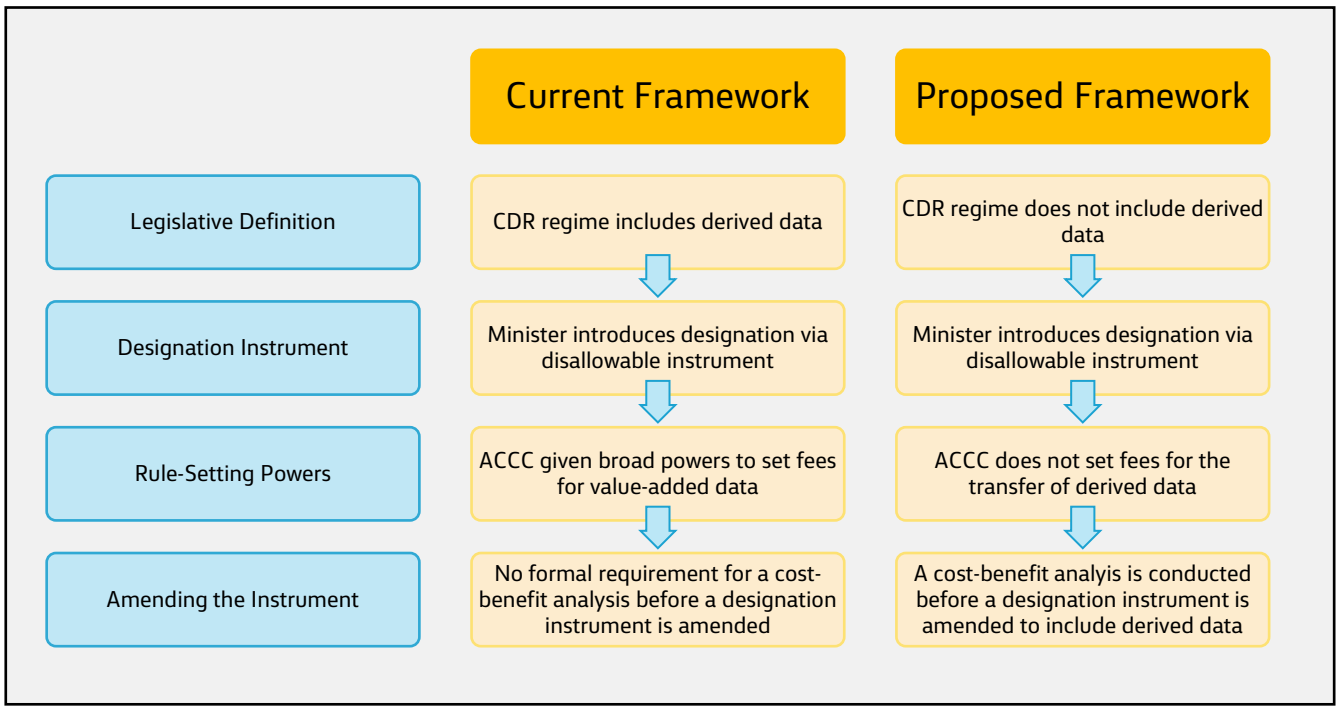

Figure 1: Schematic of Proposed changes to designation of derived data

Recommendation 2
A new, more precise, definition of CDR data should be developed by reference to principles including:

- CDR data should only include raw data and information computed from such raw data if that information: is required to make that raw data intelligible; does not result from a process of material enhancement; and will not reveal commercially confidential information (including trade secrets) of data holder if disclosed to a third party.
- 'Value added data' should be excluded from the CDR regime.

The legislation should ensure that the ACCC be required to conduct a cost-benefit analysis where new CDR data datasets are included in the CDR regime. The legislation should also allow prices to be set in the ordinary operation of the market for the provision of this derived data.

1.3 Who can access CDR data

At present, the Bill does not create any necessary link between a person who may request CDR data and the data holder from whom the data is being requested. In other words, that person need not be in a customer relationship with the data holder or have any contractual relationship with them. This is likely to lead to inappropriate disclosure obligations and uncertainties with regard to the practical application or extent of those obligations.

For example, a bank may hold information about persons that are not its customers (such as beneficial owners, directors, authorised signatories, security providers and so on). This information will be held in relation to particular customers (or prospective customers) and will not be organised or recorded by reference to the individuals or persons mentioned in, or related to, the bank's particular record.

This could lead to unintended consequences, such as a divorcing spouse being entitled to call for the disclosure of bank account details held by the bank in respect of their other partner to be disclosed as CDR data. Or a co-owner of a business in an unhappy relationship with their business partner may be able to request confidential bank data for the sole reason that that may be identified by the business name.

The Bill should be modified to require that the person requesting the CDR data must be a customer of the data holder. A wider right to cover prospective customers or non-customers (of any type) has the effect of expanding the CDR regime beyond its proposed scope, especially where the information may only need to relate in some way to the requester (regardless of the materiality of the relationship or the normal or expected entitlement of the requester to have access to that information).

Recommendation 3
Amend the definitions of CDR data and CDR consumer so that the CDR regime applies to information about a person who acquires, or has acquired, goods or services from a data holder.

2. Regulatory Powers

2.1 Designation of datasets and sectors

2.1.1 Consultation with banking sector

The Commonwealth Bank proposes that the Bill prescribe a minimum public consultation period for the Minister's making of the instruments of designation, and for the ACCC to make the Rules so as to give stakeholders sufficient time to consider and respond to complex issues arising from the designation of their sector.

2.1.2 Privacy

In order to be transparent about the privacy impact on CDR consumers of the proposed instrument of designation, the Commonwealth Bank proposes that, rather than providing the OAIC with the discretion to publish its report on the proposed instrument of designation, that the Bill mandate that the OAIC publish its report.

Recommendation 4
The Bill should provide a minimum public consultation period to provide stakeholders of potential designated sectors with the time to consider and respond to the proposed instrument of designation.

2.2 Process for designating datasets

Under the Bill, the Minister can designate classes of information which will be CDR data under the instrument of designation for a particular sector. The instrument of designation combines both the designation of specific data holders, and the datasets to comprise CDR data for that designated sector.

The Commonwealth Bank proposes that consultation be required when designating the data sets which are subject to the CDR regime. Determining the datasets in scope will require detailed consideration, given the breadth of the different products and services offered by banks and the myriad of interconnected systems within which data is generated, transferred, stored and analysed. In determining CDR data sets, the Government should have regard to cost-benefit analyses and factors such as those described in Section 1.1.

As drafted, modifying existing datasets designated as CDR data or adding new datasets to be included as CDR data for a particular sector will take a significant period of time. Therefore providing a sufficient opportunity to gather input on the designation of datasets will be of particular importance.

Once made, it appears that the Minister's instrument of designation cannot be easily amended. The Rules can set out different rules for different classes of CDR data relating to a particular sector, but cannot modify or add additional classes of information to be included in CDR data. The ACCC can make a recommendation to the Minister to vary the instrument of designation, but before making a recommendation, the ACCC must analyse the likely effect of the proposed amendment (such as likely effect on consumers, promoting data-driven innovation and the efficiency of relevant markets) and undertake public consultation.

The Bill is silent on whether the Minister can amend the instrument of designation independently and without the ACCC's recommendation. Statutory interpretation principles indicate that the power conferred by statute to make a legislative instrument also contains the power to amend or revoke the instrument which must be subject to the same conditions as making the instrument.[8]

Therefore, if the Minister independently amended the instrument of designation to add or modify existing datasets, they would still need to undertake public consultation and consider the likely effect of the proposed amendment. Nevertheless, the Commonwealth Bank proposes that the Bill expressly set out that any amendments to the instrument of designation be subject to the same public consultation process and consideration of matters set out in section 56AD.

Recommendation 5
The Bill should provide for consultation regarding the designation of classes of datasets to comprise CDR data for a designated sector. Section 56AD should set out more comprehensive factors for consideration when designating data sets.

2.3 Rule-making powers

The ACCC is conferred with extraordinarily wide powers for making the Rules for each sector. Once the Minister has designated the sector and datasets for the application of the CDR regime, the ACCC is then given the power to 'make rules' for a designated sector without any more detail or direction.

This is an unusually broad conferral of powers on a regulator. Although the ACCC has similar powers over the telecommunications sector there are more extensive provisions which specify the objectives which the ACCC must consider in making determinations.[9] In addition there are also protections for access providers under this regime in respect of pre-existing contractual rights or the nature and extent of work to be undertaken in order to grant access. No corresponding protections are provided for in the Bill.

The ACCC is not specifically required to consult with data holders in making the Rules. This disregards the recommendations of the Review into Open Banking, which stated that '*in developing the Rules, the ACCC should consult publicly to ensure that the Rules reflect the needs of the community and of industry*'.[10] The Commonwealth Bank believes that the Bill should expressly state that affected data holders be consulted on these matters, which go directly to how data holders comply with the CDR regime.

Similar data right regimes in other common law jurisdictions do not delegate such broad rule-making powers to the relevant supervisory authority. For example, in the United Kingdom:

- the Financial Conduct Authority has authority to create and publish guidance with respect to the operation of the UK regime, any matters relating to the functions of the FCA, and any other

[8] Section 33, Acts Interpretation Act 1901
[9] As part of the declared services regime in Part XIC of the Competition and Consumer Act 2010 (Cth) (CCA)
[10] Farrell, S., 2017, 'Review Into Open Banking: Giving Customers Choice, Convenience and Confidence', p.18

matters about which it appears to be desirable to give information or advice in connection with the regulations;[11] and

- the body established under the UK regime (the Payment Systems Regulator) is delegated authority for making directions and publishing guidance with respect to a narrow set of provisions under the regulations relating to provision of information about ATM withdrawal charges and the access to, and operation of, bank accounts and payment systems. Further, the Payment Systems Regulator must have regard to certain considerations, including the principle that a burden or restriction which is imposed on a person should be proportionate to the benefits which are expected to result from the imposition of that burden or restriction (see section 1.1).[12]

There are a number of sections in the Bill that set out matters that the Rules may contain, but each provision is permissive and not limiting. These sections provide that the Rules can include:

- accreditation criteria;
- the period, renewal, transfer, variation, suspension, revocation or surrender of accreditations;
- requirements that refer to the data standards;
- exemptions from complying with the requirements in the rules;
- rules requiring CDR participants to have internal or external dispute resolution processes;
- rules relating to an external dispute resolution scheme recognised by the ACCC; and
- disclosure, use, accuracy, storage, security or deletion of CDR data for which there are CDR consumers and CDR data for which there are no consumers.

While the Bill contains the Privacy Safeguards, which override the Rules to the extent of any inconsistency, the Privacy Safeguards are often drafted to allow the Rules to effectively determine their scope (see, for example, Privacy Safeguard 6).

There is no obligation on the ACCC to make Rules in respect of a sector designated by the Minister, including within any particular time period. Nor is the ACCC bound to implement Government policy, such as the Review into Open Banking which was adopted by the Government.
The Commonwealth Bank suggests that the legislation be more specific and set out in further detail the framework for how the CDR regime will operate. By way of example, such further detail should include:

- the objectives of Part IVD. The ACCC should be specifically required to have regard to those objectives when exercising its functions under Part IVD;
- limitations on the scope of the matters which the ACCC can require a data holder to undertake in disclosing CDR data should also be imposed. For example, a data holder should not be required to develop new technical capabilities except to the extent necessary to provide the CDR data.

To provide greater clarity and structure to the ACCC's rule-making power, the Commonwealth Bank proposes that the Minister be given the power to make a determination which sets out requirements with which the ACCC must comply when making the Rules. In the case of the banking sector, such a determination should require the ACCC to go no further than implementing the recommendations of the Review into Open Banking. Additionally, the Commonwealth Bank considers that the ACCC should

[11] Please see Part 9 of the *Payment Services Regulation 2017 (2017 No. 752), in particular s102 and* s120.

[12] Please see Part 10 of the *Payment Services Regulation 2017 (2017 No. 752), in particular s124, s125, s125 and 134.*

be bound by a set of principles or objectives determined by the Minister when making the Rules and should specifically be required to consult with relevant data holders.

Recommendation 6
The ACCC should be bound by a set of principles or objectives determined by the Minister when making the Rules and should specifically be required to consult with relevant data holders with respect to any such rules. For the banking sector, such a determination should be made requiring the ACCC to implement the recommendations of the Review into Open Banking.

Any report the OAIC provides to the ACCC in considering the proposed Rules should be made publicly available.

2.4 Accreditation

2.4.1 Accreditation rules

The Bill provides that accreditation of data recipients will be addressed as part of the Rules, including rules as to the period, renewal, transfer, variation, suspension, revocation or surrender of accreditation. Accreditation may be granted at different levels corresponding with different risks, including risks associated with specified classes of CDR data, specified classes of activities or specified classes of applicants.

The ACCC has broad powers to determine the substance of those Rules. The Commonwealth Bank recommends that the legislation be more specific and set out in further detail regarding baseline accreditation criteria (which requirements can then be further detailed in the Rules). That baseline criteria should be equivalent to the criteria specified under the UK regime for organisations to register as account information service providers under EU Payment Services Directive No. 2 (PSD2) which include:

- identification details – information about the applicant, such as their place of incorporation, head office and incorporated office, legal status;
- programme of operations – a description of the account information service intended to be provided and declaration that the applicant will never possess funds;
- business plan – business plan analysing the company's competitive position and description of market segments, forecast budget calculation for the first three financial years that demonstrates the applicant has appropriate resources, systems and procedures to operate soundly;
- organisational structure detailed organisational chart, overall forecast of staff numbers, description of outsourcing arrangements and use of branches and agents;
- governance arrangements and internal controls – a mapping of the risks identified by the applicant, how agents and branches are monitored, how outsourcing functions are monitored, account procedures and identity of persons for internal control functions such as compliance;
- security incidents procedure – a description of the procedure for monitoring, handling and following up on security incidents and security-related customer complaints, including organisational measures to prevent fraud, details of people responsible for assisting customers in cases of fraud, technical issues or claim management, reporting lines and contact point for customers;

- data access, logging and monitoring – description of the process to file, monitor, track and restrict access to 'sensitive payment data' (datasets which can be used to carry out fraud such as personalised security credentials);
- business continuity arrangements – business impact analysis, identification of back-up site and explanation of how the applicant will deal with significant continuity events and disruptions;
- security policy – a detailed risk assessment and security control and mitigation measures to protect against the risks identified and a description of the IT systems;
- director and key management identification and assessment of suitability – personal details of the directors and responsible persons for management of the applicant, including evidence of knowledge skills and experience and evidence of reputation, honesty and integrity and any information on investigations, enforcement proceedings or sanctions that a person has been involved in;
- professional indemnity insurance and/or bank guarantee – evidence of professional indemnity insurance and/or comparable guarantee for a specified amount in the Rules; and
- compliance with security guidelines specified in the data standards.

To further ensure the integrity of the CDR regime, the Commonwealth Bank recommends that the accreditation rules require accredited data recipients:

- to provide evidence and assurance regarding the security of IT systems and the technical, organisational and contractual measures implemented with IT service providers, comprising the accredited data recipient's IT infrastructure;
- be subject to enhanced due diligence, including financial due diligence and background checks for the employees of the entity that will be handling CDR data as an accredited data recipient, such as is required by anti-money laundering legislation; and
- be insured for liabilities to ensure solvency for remediation purposes.

2.4.2 Non-accredited data recipients

The Bill anticipates the making of the Rules whereby CDR data that does not relate to a CDR consumer can be disclosed to non-accredited recipients. The Commonwealth Bank considers that enabling a CDR regime which permits rules of this nature is inappropriately broad. While some information - such as publicly available information product features, fees or charges - may be capable of being disclosed more broadly, as a general proposition the Bill should not depart from an accreditation-based sharing regime which engenders trust in the system. The Bill should define with more precision the data which may be exempt from accreditation.

Recommendation 7
The Bill should determine non-exhaustive baseline accreditation criteria (such as those set out in section 2.4) for the banking sector which should contain requirements to ensure recipients have sufficient resources and processes and appropriate management as a prerequisite to being trusted with CDR data.

The Bill should distinguish between datasets that can be disclosed to non-accredited recipients and datasets that cannot. This could be dealt with by Ministerial determinations or other instruments issued on a sector by sector basis.

3. Principles of Reciprocity

Robust principles of reciprocity will maximise the value of the Open Banking regime and eliminate 'free rider' dilemmas for participants. It will also maximise the benefit of the consumer data right to consumers, as they will have no barriers to sharing data at their request. This means that new participants who enter the CDR regime to access consumer data should be required to share equivalent data with other CDR participants, if a consumer so wishes.

The obligation to disclose CDR data will be set out in the Rules, but section 56BC clearly contemplates that any such disclosure obligations will be limited to CDR data. It does not impose any obligations on an accredited data recipient to make any data available under Part IVD, unless that data is CDR data.

Recommendation 3.9 of the Review into Open Banking stated '*Entities participating in Open Banking as data recipients, should be obliged to comply with a consumer's direction to share any data provided by them under Open Banking, plus any data held by them that is transaction data or that is the equivalent of transaction data*'.[13] The Commonwealth Bank has consistently supported reciprocity on the basis that mutual data-sharing is likely to lead to a more vibrant and dynamic data sharing economy.

Without this principle of reciprocity, the Consumer Data Right becomes a 'one-way' transfer of data, which greatly limits the potential benefits envisaged by the CDR regime. The CDR regime will operate in the best interests of consumers if the Rules require data recipients, as a part of attaining accreditation, to make available the data which they collect as part of providing goods or services to CDR consumers. The Rules should provide a mechanism for determining equivalent datasets as part of the accreditation and on-boarding process, including the requirements to make that data available and the appropriate rules to be an accredited recipient of that data.

Accreditation would be contingent on determining equivalent datasets and implementing processes to make equivalent datasets available to the transmitting data holders.

Recommendation 8
The Government should further consider the reciprocity principle outlined in the Review into Open Banking in order to encourage greater usage of the CDR regime for the benefit of consumers and to further encourage and stimulate innovation and competition across markets.

The Bill should reflect the principle that any accredited data recipient should be under an obligation to make data generated or held by that recipient from goods or services supplied to a CDR consumer available as CDR data to data holders and other accredited data recipients.

[13] Farrell, S., 2017, 'Review Into Open Banking: Giving Customers Choice, Convenience and Confidence', p44

4. Consumer Data Security

Maintaining CDR data security is vital in building trust and confidence in the Consumer Data Right and will be a key driver of its take-up over time. A robust and proportionate approach to CDR data security will ensure that the industry avoids developing 'weak links' in Australia's cyber security infrastructure.

4.1 'Reasonable Steps' threshold

The Rules should include safeguards against the disclosure of CDR data to accredited data recipients in certain circumstances, rather than this being a provision which the ACCC may optionally include in the Rules. These safeguards could include exemptions from disclosure of CDR data by data holders:

- to accredited data recipients that no longer meet the accreditation criteria (including not maintaining appropriate security standards), whose accreditation has been suspended or varied or revoked, or where the data holder reasonably suspects the accredited data recipient has suffered an unauthorised disclosure of CDR data; and
- in emergency circumstances, such as a security breach of one or more CDR participants that is substantially affecting the operation of CDR regime for the banking sector.

These exemptions are necessary for the protecting the security of CDR data for CDR consumers and to preserve the integrity of the CDR regime.
Market participants will undertake monitoring of cyber risks and respond to emerging threats in real-time, which can be a challenge for regulators. Recognising this, the recent *Mandatory Comprehensive Credit Reporting Bill (2018)*, at section 133CR, includes provisions for organisations to withhold the supply of data to third parties who are found not to have taken 'reasonable steps' under section 20Q of the Privacy Act to secure their customer's data online. These provisions also contain penalties for organisations who withhold the supply of data from third parties, where the third party is found to have taken 'reasonable steps' under the Privacy Act.

Recommendation 9
The Rules should include safeguards against the disclosure of CDR data to accredited data recipients in certain circumstances, rather than this being a provision which the ACCC may optionally include in the Rules. These safeguards could include exemptions from disclosure of CDR data by data holders:

- to accredited data recipients that no longer meet the accreditation criteria (including not maintaining appropriate security standards), whose accreditation has been suspended or varied or revoked, or where the data holder reasonably suspects it has suffered an unauthorised disclosure of CDR data; and
- in emergency circumstances, such as a security breach of one or more CDR participants that is substantially affecting the operation of CDR regime for the banking sector. These exemptions are necessary for the protecting security of CDR data for CDR consumers and to preserve the integrity of the CDR regime.

Further, the Bill should include provisions for data holders to withhold the supply of data to accredited data recipients who have not taken 'reasonable steps' to secure their customer's data or CDR data.

4.2 Recognition of industry standards

Many of the sectors which are slated for designation, including the banking sector, are already subject to complex regulation including via industry codes and standards. The Commonwealth Bank is concerned that the Bill does not make provision for the consideration of those industry codes or standards in the designation of sectors and CDR data or in the making of Rules and data standards. In particular, the Commonwealth Bank is concerned that the CDR regime may place obligations on data holders and accredited data recipients which may be inconsistent with existing regulation.

By way of example, APRA has released a draft of a proposed prudential standard on information security: see the draft Prudential Standard CPS 234 Information Security. The proposed standard is a response to the growing threat and potential financial impact of cyber-attacks. The proposed standard's stated objective is to minimise the likelihood and impact of information security incidents on the confidentiality, integrity, or availability of information assets, including information assets managed by related parties or third parties.

Recommendation 10
Sector regulation, mandatory Prudential Standards and generally applicable industry standards should be consulted at all steps of the CDR process – from designation, to determining the Rules, to considering the application of protections such as the privacy safeguards.

To the extent of any conflict or inconsistency between such standards or regulation and any of the privacy safeguards, instrument of designation, Rules, and data standards, mandatory Prudential Standards or other sector regulation should take precedence.

5. Participants in a CDR regime

The creation of separate obligations for data holders and accredited data recipients under the CDR regime will cause unnecessary regulatory complexity and lead to a set of potentially inconsistent obligations for CDR participants who may be both data holders and data recipients for different CDR datasets.

As such, the Commonwealth Bank believes that many restrictions on the collection, use and disclosure of CDR data can be applied consistently to both data holders and accredited data recipients.

5.1 Data Holders

The Bill defines a data holder as a person or a class of persons that is specified under the instrument designating the sector to which the CDR regime will apply and holds CDR data (other than because of a disclosure under the CDR regime of the CDR data). The Bill allows for the Rules to modify the condition that a person is not a data holder because they are holding CDR data as a result of a disclosure under the CDR regime of the CDR data. This means that the Rules can allow accredited data recipients to be data holders and vice versa. This would seem to be an appropriate and necessary element of the regime.

The Bill's definition of data holder will capture data which a data holder generates when it is providing services such as white-labelling. Experience of the mandatory data breach notification scheme where more than one person can be required to comply with the same requirement for the same data creates confusion and difficulties for both business and the consumer. As such, the Commonwealth Bank considers it is more appropriate for one party to assume the obligation to transfer data, and it would seem logical that this is the party with whom the consumer has the relationship.

There is no scope in the Rules for the ACCC to amend the persons or class of persons specified in the instrument of designation made by the Minister (essentially, the data holders), nor the class of information specified in an instrument designating a sector (essentially, the CDR data). This means that the persons or class of persons specified in the instrument that can qualify as data holders within section 56AG of the Bill will remain unchanged unless the instrument of designation is amended (which the ACCC may recommend to the Minister after consulting with the public and considering matters such as its likely regulatory impact and effect on consumers).

5.2 Accredited Data Recipients

The Bill defines an accredited data recipient as: a person who holds accreditation under the CDR regime; holds particular CDR data that was disclosed to it under the Rules; and the person is not a data holder of the CDR data. The effect of this is that a person cannot be both a data holder and an accredited data recipient of a designated dataset.

A person can, however, be a data holder with respect to one dataset and an accredited data recipient with respect to a different dataset. This may cause issues where an accredited data recipient has been provided with a CDR dataset outside of the CDR regime (such as a customer's contact details) and also receives the same dataset as a result of a disclosure by a data holder under the CDR regime (for

example, the bank transfers the entire customer record which will include a customer's contact details in accordance with section 56EI to a fintech).

In this situation, an accredited data recipient could potentially have inconsistent sets of obligations as a data holder and a data recipient under the CDR regime. For example, under Privacy Safeguard 11, an accredited data recipient must destroy or de-identify the CDR data that is no longer needed for the purposes permitted under the Rules. However, the Australian Privacy Principles (**APPs**) only require an entity to destroy or de-identify personal information that it no longer needs for any purpose.

If a data recipient is also a data holder with respect to a CDR dataset, then it would potentially be permitted to retain the CDR dataset under the APPs as a data holder, even though it would also be required to destroy or de-identify the CDR dataset as a data recipient. To avoid an inconsistent set of obligations under the regime, we propose that protections around the collection, use and disclosure of CDR datasets be applied consistently to both data holder and accredited data recipients.

Further, it will be difficult for a person that is both a data holder and data recipient for CDR datasets to comply with potentially inconsistent obligations where data has been co-mingled. For example, in the banking sector, it will be extremely difficult to treat data collected in a loan application outside the CDR regime which the bank holds as a data holder, separately to information about a customer's spending habits that the bank receives from a fintech.

5.3 Application of the CDR to corporate groups

The Bill primarily imposes obligations on data holders and accredited data recipients which are legal persons, including natural persons and corporations. There is no section in the Bill which expressly deals with related bodies corporate or corporate groups. The effect of this is that each company within a corporate group will have separate rights and obligations provided for under the Bill, unless the Rules deal with this point. For example, one company in a corporate group may qualify as a data holder or an accredited data recipient (such as an ADI) but other companies within the group will not. The Commonwealth Bank is supportive of the Bill's objective for each related body corporate to be separately subject to the CDR regime, although it considers that the Bill and the Rules should contain some exemptions, including for the disclosure of CDR data between related bodies corporate and for related bodies corporate to meet certain accreditation criteria, where another group company is a data holder.

The accreditation regime in the Bill for accredited data recipients currently applies to a person, which means that each related body corporate of an accredited data recipient will need to become an accredited data recipient itself and obtain a request from a CDR consumer for CDR data to be transferred to them before they register for accreditation to receive all CDR data (see our comments on the effect of Privacy Safeguard 6 in Section 6). This may create unnecessary compliance costs and burdens if a data holder's related bodies corporate which share the same security controls as the data holder are required to undergo an accreditation process. The Commonwealth Bank suggests that the Rules include exemptions for the satisfaction of accreditation criteria for related bodies corporate of data holders sharing the same IT systems and functionality.

Recommendation 11
The relationship between data holders and data recipients and their obligations should be clarified.

Limb (d) of the definition of accredited data recipient should be deleted to take into consideration that a person may be both a data holder and an accredited data recipient with respect to some datasets. The obligations on data holders and data recipients in respect to protection of CDR data should be the same.

The Rules should provide for the modification of the accreditation regime for accredited data recipients so that there are appropriate exemptions from the accreditation requirement for related bodies corporate which share the same accredited IT systems with the accredited data recipient.

5.4 Application of the CDR to foreign entities

The Bill does not provide a test for determining when CDR data will be generated or collected in Australia. The Explanatory Memorandum to the 2014 Privacy Act notes that (and the OAIC as privacy regulator adopts this position in applying the Privacy Act) wording regarding the collection of personal information 'in Australia', means the personal information is collected from an individual who is physically present in Australia. This interpretation may inform the approach to interpreting 'generating or collecting CDR data in Australia', such that it relates to a natural person physically present in Australia. It may by extension apply to companies which are CDR consumers and which are carrying on business, or which are resident or domiciled in Australia.

In order to be a 'data holder' to which Part IVD would apply, that person must either be specified or belong to a class that is specified in the Minister's instrument designating that sector. It is possible that such a designation for the banking sector will be made in respect of particular corporate entities – as such, any off-shore subsidiaries would be automatically excluded as data holders. However, in the event that offshore subsidiaries are captured by the designation, they would only be considered a data holder to the extent that they hold CDR Data, which as described above, requires the relevant nexus with Australia.

The extent of the nexus of the offshore company with Australia will determine how problematic this issue will be in practice. For example, if a subsidiary of the Commonwealth Bank uses the Commonwealth Bank's technology located in Australia to operate its business, it is conceivable that the relevant data recorded and manipulated using that technology will be CDR data. Alternatively, an offshore Commonwealth Bank subsidiary which is in the class of persons designated as a data holder and which provides services to individuals or businesses in Australia will satisfy the geographical scope requirements of the Bill.

Foreign entities may also be subject to accredited data recipient obligations under the Bill if those entities become accredited data recipients. Note 2 of section 56AH expressly states that a foreign entity may be an accredited data recipient of CDR data under the Rules. Under section 56CE, a foreign entity may be accredited if it satisfies the criteria specified in the Rules for accreditation. This means that unless the Rules impose a nexus test with Australia, a foreign entity that has little or no presence in Australia could become an accredited data recipient and receive CDR data.

Section 56AH(1)(b) makes clear that foreign entities will be subject to accredited data recipient obligations if they receive CDR data that has not been generated or collected in Australia, but is subject to the regime because the entity collecting or generating the CDR data is an Australia company or body corporate registered with ASIC.

Even though foreign entities could be subject to obligations under the CDR regime as data holders or accredited data recipients, from a practical perspective, it will be difficult for the ACCC and OAIC to exercise enforcement powers against an entity with little or no presence in Australia. It could be particularly difficult to obtain quick and legally binding injunctive relief ordering the data holder or accredited data recipient to do, or to refrain from doing, a particular act. In addition, some enforcement powers of the ACCC and OAIC such as requiring a person to attend hearings, will be ineffective in respect of foreign entities that do not have representatives in Australia.

It is possible that the difficulties with enforcement of foreign judgements could be addressed by requiring offshore companies to register under the *Corporations Act 2001* (Cth) and to be required to provide security for performance such as a bank guarantee or performance bond, although consideration would need to be given to which regulatory body under the regime any such security would be provided.

The Bill's extraterritorial application is different to the Privacy Act, in that the Privacy Act contains a pre-requisite for the foreign entities to 'carry on business' in Australia before they can be subject to the Privacy Act, notwithstanding that they have collected or held personal information in Australia. In the Bill, the CDR regime will apply to foreign entities so long as CDR data is generated or collected in Australia. Depending on the scope of the phrase 'generated or collected in Australia', the Bill could apply to foreign entities that do not carry on business in Australia.

The effect of this is that it will be more difficult to enforce the CDR regime against foreign entities that have little to no presence in Australia. Furthermore, if foreign entities have been designated or belong to a class of persons specified in the Minister's instrument of designation, they will be data holders under the CDR regime, but will not need to comply with the APPs if they do not 'carry on business' in Australia. Consequently, CDR data in the hands of foreign entities that are data holders but not subject to the Privacy Act, will only be subject to the protections in the Privacy Safeguards and not the APPs. To ensure that CDR data is subject to the same level of protection as will be required of data holders (whether they carry on business in Australia or not), the extraterritorial application of the Privacy Act should be modified to apply to foreign entities which are CDR participants.

Recommendation 12
The meaning of generated or collected in Australia should be further clarified in the Bill.

Foreign corporations without an appropriate presence in Australia should not be permitted to be accredited data recipients.

The extraterritorial application of the Bill should align with the extraterritorial application of the Privacy Act, such that foreign entities which are CDR participants should be subject to the Privacy Act.

6. CDR Privacy Safeguards

Privacy and trust are critical to the success of Open Banking and the Consumer Data Right. The Commonwealth Bank supports strengthening consumer privacy safeguards to ensure consumer information is handled appropriately. To the extent possible, this should align with existing safeguards, such as those included in the Privacy Act and should be designed to reduce complexity for both consumers and participants.

6.1 The Scope of the Privacy Safeguards

The CDR explanatory memorandum suggests that the Privacy Safeguards are intended to substitute the APPs for accredited data recipients only when handling the CDR data transferred on request by the CDR consumer; however, the Commonwealth Bank is concerned that the Privacy Safeguards, as currently drafted, do not achieve the Government's stated objectives.[14]

The Commonwealth Bank suggests that the scope of the Privacy Safeguards be reconsidered to reduce complexity and to avoid significant extensions of privacy law which would appear to not be necessary.

The CDR explanatory memorandum provides examples which suggest that a data holder's collection, use, storage and disclosure of personal information will be subject to the APPs and will only become subject to the Privacy Safeguards for the purpose of disclosing to an accredited data recipient.[15] That accredited data recipient will then be bound by the Privacy Safeguards and not the APPs, unless and until the accredited data recipient commences providing services to the consumer.[16] However, the Commonwealth Bank is concerned that the Bill does not reflect that level of precision and clarity regarding the application of the Privacy Safeguards.

As currently drafted, the Privacy Safeguards are designed to be a modified version of the APPs which apply to the handling of CDR data and apply to the handling of such CDR data as is information relating to an identifiable CDR consumer including any entity which is not a natural person. They are not limited in application in the manner suggested by the explanatory memorandum – rather they could be taken to apply to limit the ability of a data holder to deal with CDR data in a manner which is consistent with the APPs.

CDR data which is personal information under the Privacy Act will already be required to be handled in accordance with the Privacy Act and this will continue with the enactment of the Bill. Understandably though, it is necessary to ensure that CDR data:

- may be transferred by a data holder to an accredited data recipient (or other permitted party) without breaching other laws;
- that an accredited data recipient be required to only collect CDR data with the consent of the CDR consumer; and
- that an accredited data recipient only be permitted to use and disclose CDR data in accordance with the consent provided by the CDR consumer.

[14] Exposure Draft Explanatory Materials, Treasury Laws Amendment (Consumer Data Right) Bill 2018, at 1.169
[15] Ibid, examples 1.14 and 1.15
[16] Ibid, example 1.14

The Commonwealth Bank believes that the current Privacy Safeguards create greater complexity than is required to achieve important protections for consumers who chose to share information under the regime. Addressing the relatively straightforward requirements above is what is necessary to protect the interest of CDR consumers, provided the Rules make clear how consents must be obtained (unbundled and express) and any restrictions considered appropriate on the scope of the consents which may be obtained are dealt with.

The Commonwealth Bank submits that to impose a different and overlapping set of principles for the handling of information is unnecessary and goes further than the Government's stated objectives in addressing the relevant issues and the intentions set out in the explanatory memorandum. Furthermore, the expansion of principles designed to protect the right of a natural person to privacy by controlling the handling of their personal information to include business information is a significant departure from international norms. It is suggested that such an outcome is perhaps inadvertent as it has never been previously considered as a policy objective of the consumer data rights reform and does not appear a necessary part of that reform.

Given this, the Commonwealth Bank submits that the Privacy Safeguards be amended to reflect the essential protections required for CDR consumers. Additional comments are provided on the Privacy Safeguards in the sections immediately following.

6.2 Overlap between APPs and Privacy Safeguards

The Privacy Safeguards apply to protect information which is personal information under the Privacy Act. This will have the effect that for CDR data which is personal information, a CDR participant will need to handle personal information in accordance with both the Privacy Act (including the APPs) and also the Privacy Safeguards. This will create implementation and compliance complexity.

There are other likely consequences arising from this overlap. A breach of the Privacy Safeguards and the APPs arising from the same conduct could result in:

- enforcement action being brought by the OAIC under the Privacy Act;
- enforcement action being brought by the ACCC or the OAIC under Part IVD of the CCA; and
- claims by aggrieved individuals or the ACCC for court orders in respect of compliance with the data standards.

This could also create exposure to liability for claims under the different enforcement regimes in respect of the same conduct. This will be further discussed in **Section 7**.

6.3 Privacy Safeguard 6 - Use or Disclosure of CDR Data

This Privacy Safeguard could create issues with use and disclosure rights of CDR Data in the ordinary course of business once a CDR consumer exercises rights to request a transfer of CDR data.

Privacy Safeguard 6 provides that if the Commonwealth Bank has received a request for a transfer of CDR data then it must not disclose the CDR data (or associated data) unless disclosure is required or authorised under the Rules; or, if required or authorised by law, other than the APPs. Given the exclusion of the APPs, once the Commonwealth Bank has received a transfer request, the right the Commonwealth Bank has under the APPs to disclose CDR data which is personal information, such as for the primary purpose of collection for a reasonably related secondary purpose no longer apply. The

right to transfer personal information (but not other CDR data) between related bodies corporate under Section 13 of the Privacy Act remains.

The result of this approach would be that unless Privacy Safeguard 6 is limited to a disclosure in response to a request by a CDR consumer, a data holder would be prohibited from using and disclosing requested CDR data to conduct its business but a related body corporate to whom it transferred such information would not be subject to these restrictions.

6.4 Privacy Safeguard 7- Direct Marketing

This Privacy Safeguard allows an accredited data recipient to use or disclose CDR data (including derived data) to direct market to CDR consumers if the use is in accordance with a valid consent from a CDR consumer or the use or disclosure is required or authorised by or under an Australian law, other than the Australian Privacy Principles.

Unlike APP 7 (Direct Marketing) this Privacy Safeguard does not deal with the interaction with other legislation such as the *Spam Act (2003)* and *Do Not Call Register Act (2006)*. Consequently, as drafted, Privacy Safeguard 7 would permit the use or disclosure of CDR data to direct market consumers if authorised under the Spam Act. As the Spam Act allows organisations to send electronic messages for direct marketing purposes based on implied consent, this would undermine requirements for express consent under the Rules. We note that the Explanatory Memorandum states that it expects the Rules to mandate obtaining express consent for disclosures of CDR data. To preserve the threshold of express consent for disclosures of CDR data, Privacy Safeguard 7 should exclude the *Spam Act (2003)* from applying to authorise the use or disclosure of CDR for direct marketing.

6.5 Privacy Safeguard 8 - Cross-border disclosure of CDR Data

The drafting of Privacy Safeguard 8 suggests that a foreign entity that is not accredited under the CDR regime could get access to CDR data on request by a CDR consumer if conditions specified in the Rules are met.

The Government does not seem to have intended that Privacy Safeguard 8 operates in this way, as the explanatory memorandum states that CDR data must only be provided to overseas entities if they are an accredited data recipient.

Privacy Safeguard 8 also doesn't appear to contemplate the profile of data holders' or accredited data recipients' information technology infrastructure and the likelihood that such infrastructure, particularly for larger or global organisations, will involve the use, disclosure and hosting of data, including CDR data, off-shore.

Cross-border disclosure of CDR data to, and use by, suppliers for the provision of IT services or outsourcing arrangements within a data holder's or accredited data recipient's IT infrastructure should be governed by the Privacy Act (regarding personal information) and the accreditation regime (regarding implementation of technical, organisational and contractual security measures).

6.6 Privacy Safeguard 10 - Quality of CDR Data

This Privacy Safeguard imposes an obligation on a CDR participant who would reasonably be expected to be aware that some or all of the CDR data that it discloses under the CDR regime is incorrect, to inform each CDR consumer for the CDR data accordingly and do so in writing. This safeguard is problematic in that it does not provide exceptions where CDR consumers have already been informed of the inaccuracy of their CDR data by another person, and does not allow a CDR participant to pass on their obligation to inform a CDR consumer to a third party (who may or may not be a CDR participant).

In a white-label arrangement, it may be more appropriate for another organisation that has the customer-relationship with a CDR consumer to inform them of the incorrectness of their data, rather than the data holder. We recommend that Privacy Safeguard 10 contain exceptions to provide for all types of commercial arrangements in a CDR-designated sector.

Recommendation 13

The Government should re-consider the purpose for introducing the Privacy Safeguards with a view to reducing the number of safeguards to only those permitting disclosure by a data holder to a data recipient and regulating collection, use and disclosure of CDR data by an accredited data recipient.

The Privacy Safeguards should not restrict or prevent any use of CDR data by the data holder which would otherwise be permitted.

Privacy Safeguard 6 should be modified so that it only applies to the actual disclosure by a data holder of CDR data in response to a request by the relevant CDR consumer.

Privacy Safeguard 7 should be modified to exclude the Spam Act from applying to authorise the use or disclosure of CDR data for direct marketing.

Privacy Safeguard 8 should be modified:

- so that CDR data can only be disclosed on the request of a CDR consumer to a foreign data recipient that is accredited under subsection 56CE(1) of the Bill and the conditions specified in the Rules are met (in other words, substitute 'or' after subsection 56EK(c) to 'and');
- to ensure that data holders and accredited data recipients are not restricted, or subject to conflicting obligations, with respect to using off-shore service providers as part of their information technology infrastructure; and
- to ensure that cross-border disclosure of CDR data to, and use by, suppliers for the provision of IT services or outsourcing arrangements within a data holder's or accredited data recipient's IT infrastructure are governed by the Privacy Act (regarding personal information) and the accreditation regime (regarding implementation of technical, organisational and contractual security measures).

Privacy Safeguard 10 should be amended to contain exceptions to inform CDR consumers that include:

- where CDR consumers have already been informed the CDR data was inaccurate, out-of-date or incomplete;
- where a third party will assume the obligation to inform the CDR consumer; or
- where the data holder, despite taking all reasonable steps to keep CDR data up to date, complete and accurate, does not have the current contact details of the relevant CDR consumer to inform them.

7. Consistency with other regulatory regimes

7.1 Privacy Act and CCR Bill

Under Part IIIA of the Privacy Act, credit providers are subject to express limitations on the extent to which they can disclose and share 'credit eligibility information' about an individual. Those limitations are not recognised in the Bill, with the result that a data holder that is a credit provider may find themselves subject to conflicting obligations with regard to the disclosure and non-disclosure of the same information.

In the case of a bank, or any other credit provider, the credit provider will only be permitted by Part IIIA of the Privacy Act to disclose 'credit eligibility information' where it can do so in a manner authorised by one or more of sections 21J, 21K, 21L, 21M or 21N of the Privacy Act. Currently, the Bill takes no account of such conflicts. It is not appropriate to leave it to the Rules to resolve or avoid the potential conflict of legal obligations.

Under the CCR Bill, it is proposed to require large ADIs to provide 'mandatory credit information' to 'eligible credit reporting bodies'. The CCR Bill also proposes to regulate the circumstances in which those credit reporting bodies may disclose the mandatory credit information (or information derived from that information) to other persons.

The Bill does not consider the interaction between the CDR and the separately proposed *National Consumer Credit Protection Amendment (Mandatory Comprehensive Credit Reporting) Bill 2018* (**CCR Bill**). If CDR consumers are authorised to direct the provision of any information related to them to an accredited data recipient (where the data holder is a credit provider) the CCR Bill may become redundant. It is recommended that, at a minimum, 'credit eligibility information' within the meaning of the Privacy Act and 'mandatory credit information' within the meaning of the CCR Bill should not be subject to any disclosure obligations under the separate disclosure regime proposed by the Bill.

Recommendation 14
The disclosure of credit eligibility information and mandatory credit information should not be authorised by the CDR Bill or potentially authorised under the Rules on the basis that the Part IIIA of the Privacy Act and the CCR Bill are specifically designed to address credit eligibility information and mandatory credit information

8. Dispute Resolution

The accessibility and enforcement of external dispute resolution schemes is an essential consumer protection, and fundamental to the operation of the Consumer Data Right. These schemes should be recognised by the ACCC for the resolution of disputes between CDR participants, to reduce the regulatory burden and provide an accessible, low-cost avenue for consumers to seek redress.

8.1 Recognition of foreign external dispute resolution schemes

The process for recognising an external dispute resolution scheme is not subject to disallowance or parliamentary review.

Under section 56DA of the Bill, the ACCC has the power to recognise an external dispute resolution scheme through notifiable instrument for the resolution of disputes of the following nature:

- about the operation of the Rules for one or more designated sectors; and
- disputes between one or more data holders or accredited data recipients or CDR consumers, or other persons relating to any designated sector.

Given that some dispute processes may be more appropriate than others, and the potential for the parties to be required under the Rules to use those processes, the Commonwealth Bank suggests that the ACCC to be required to consult with stakeholders before recognising an external dispute resolution scheme . Additionally, the recognition should be a disallowable instrument.

An external dispute resolution scheme is not defined in the Bill and there is not an existing definition in the CCA. It is not clear from the wording in the Bill whether the ACCC can recognise foreign dispute resolution schemes.

It is possible that foreign external dispute resolution schemes could be chosen by the ACCC to apply to disputes involving an accredited data recipient or data holder that is a foreign entity. If a foreign entity is subject to an external dispute resolution scheme in the country in which it has its main office or establishment, then this scheme may be recognised by the ACCC or it may apply on its face to resolve CDR disputes of the relevant entity. The Commonwealth Bank reiterates its recommendation 8 that the Government re-consider whether foreign corporations without a presence in Australia should be permitted to be accredited data recipients.

The explanatory memorandum to the Bill lists external dispute resolution schemes within Australia, specifically AFCA, the Telecommunications Industry Ombudsman, the State and Territory Energy Ombudsman and states that the CDR regime intends to leverage these existing schemes when appropriate. This appears to indicate that the intention of Parliament is to recognise Australian-specific external dispute resolution schemes.

Recommendation 15
The ACCC should be limited to only recognise Australian external dispute resolution schemes when exercising its power under s56DA(1) of the Bill.

9. Liability and enforcement

The Bill contains provisions providing a shield from civil or criminal liability for a CDR participant who acts in accordance with the regime, which is necessary in order for the CDR regime to be able to operate. The provisions protecting CDR participants from liability need to apply at all times (with a carve-out for any particular breach) and with an appropriate burden of proof.

9.1 Status of Data Standards for enforcement purposes

The Bill provides for data standards that will complement the Rules made by the ACCC and facilitate the sharing and use of the consumer data that is subject to the CDR to be made by the Data Standards Chair (appointed by the Minister). The data standards will prescribe the format of data, method of transmission and security requirements. If a data holder is unwilling or unable to provide the designated data in a format consistent with the data standards, then the party seeking the information may seek redress.

If a data holder or accredited data recipient fails to meet the data standards, the following enforcement action may occur:

- **Contractual enforcement:** The data standards will operate as a multi-lateral contract between each data holder and each accredited body under which each party agreed to observe the data standards to the extent those standards apply to them and engage in any conduct required by the Data Standard (s56FF CCA);
- **Enforcement by 'aggrieved parties':** Any person aggrieved by a failure to meet a data standard may apply to the court to enforce that Data Standard (s 56FG); and
- **Enforcement by ACCC:** The Bill also enables the ACCC to seek enforcement of data standards by a court.

The use of a statutory contract to enable enforcement between data participants may over-complicate the enforcement mechanism. Company constitutions are another instance where a statute deems a contract to exist and that mechanism has generated significant case law debating which interpretive rules should be applied in the circumstance where a contract is deemed to exist, but the parties to that contract did not agree to the bargain (and therefore important contractual elements such as intent are absent).

Further, this form of private rights enforcement mechanism when adopted elsewhere (including under the CCA) has been vulnerable to tactical litigation by one competitor against another for its own commercial benefit. To avoid this outcome, the regime would benefit from a materiality threshold to trigger a claim. Such a threshold should require both the breach and the impact of that breach to be material.

9.2 Powers of the ACCC and OAIC for regulating the CDR regime

Any dispute resolution processes and enforcement processes which apply to the CDR regime should be clear and minimise the potential for multiple processes to be run simultaneously in relation to the same dispute.

The Bill proposes to extend the existing CCA enforcement regime to cover the new Part IVD of the CCA. However, it is unclear what civil penalties may be applied to breaches of the Rules and in what circumstances, as those penalties are to be the subject of the Rules themselves. The consumer data right (while applying to a wider class of persons) is related to the rights afforded to individuals under the APPs.

It is intended to create mechanisms to obtain access to information about a person. Given this similarity, the Commonwealth Bank considers the civil penalty regime of the Privacy Act is the appropriate and comparable benchmark to adopt.

The Bill also provides a significant right for the ACCC to delegate its functions and powers as follows:

- any of its functions and powers under Part VI and s155 to the OAIC; or
- any of its function and powers under s155 that relates to a contravention or potential contravention of Part IVD or the Rules to any person who the ACCC considers has appropriate qualifications or expertise to perform that function or power.

It is unusual for a piece of legislation to provide for multiple regulators to have the same enforcement powers, and to also to enable the ACCC's significant powers to compel the production of documents and information under s155 to be delegated to 'any person'. This could lead to unintended confusion as to which regulator is responsible for a particular matter, and could give rise to inefficiencies.

9.3 Liability for Compliance with Rules and Data Standards

The Bill contains a provision providing a shield from civil or criminal liability for a CDR participant, which the Commonwealth Bank agrees is a prerequisite in order for the CDR regime to be able to operate.

However, the liability shield only applies in the event the CDR participant complies with all of Part IVD, any regulations made for the purpose of Part IVD and the Rules. In addition, a CDR participant bears an evidential burden of pointing to evidence that it does so comply in order to rely on the shield.

The Commonwealth Bank is concerned that a breach of one provision of, say, the Rules could then operate to expose CDR participants to claims which arise in respect of other matters which the liability shield was drafted to prevent. It also believes that it is unreasonable burden on any CDR participant for it to bear an evidential burden of seeking to prove it is in compliance with all relevant laws, given that a CDR participant would need prove its compliance with each requirement in the Rules, the Privacy Safeguards and any regulations made for the purpose of Part IVD. For example, the data standards may prescribe a protocol that is superseded by developments in new technology or industry practice. An unduly narrow view of compliance with a versioned standard will have the unintended effect of exposing data holders to liability where industry best practice evolves faster than the data standards. Further, there could be a trivial breach of a reporting requirement which then exposes a data holder or accredited data recipient to civil or criminal liability for unrelated offences which arise from the structure of the CDR regime, which requires the sharing of information between competitors.

Recommendation 16

The enforcement of data standards against both data holders and any recipient of data under the CDR regime be simplified by being undertaken by the ACCC. This would be effected by:

- removing the provisions deeming data standards as multi-lateral contracts;
- introduction of a materiality threshold to trigger the right for aggrieved persons to bring enforcement proceedings for material breaches of the data standards.

The Bill should provide:

- for the civil penalty regime to be applied in respect of the proposed Part IVD of the CCA is the civil penalty regime contained in the Privacy Act; and
- the power for the ACCC to delegate functions and powers be removed.

The Bill should:

- provide for the liability shield to remain unaffected except if a person breaches Part IVD, the regulations made for the purpose of Part IVD or the Rules, then that person would be liable for a breach of that specific provision; and
- be amended by removing the burden of proof requirement for those seeking to rely on the liability shield.