16 October 2018

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

Via Email: data@treasury.gov.au

Commonwealth Bank welcomes the opportunity to respond to the Treasury Laws Amendment (Consumer Data Right) Bill 2018: Provisions for further consultation.

Commonwealth Bank broadly supports the suggested amendments in the revised legislation, including: limiting the scope of rule-making powers; clarifying the interaction between the *Privacy Act 1988* (Cth) (**Privacy Act**) and the Safeguards; clarifying reciprocity as a key element of the CDR regime from its commencement; further consultation requirements ahead of sectoral designation; and the clarification of rule-making powers in regards to data access and use.

The comments in this submission relate to matters of implementation and the efficiency of the regime once it is established, not the policy intent itself.

As noted in our previous submission, Commonwealth Bank is proud to be one of the first organisations in Australia who will make the Consumer Data Right a reality for our customers and we recognise the importance maximising the benefits of the regime for all Australians.

Contents

Summary of Recommendations

Recommendation 1

Commonwealth Bank considers that the Treasury can achieve its intent, benefit consumers, and ensure investment certainty and innovation in the data economy by amending the definition of CDR data to capture the principles that CDR data is information:

- that is specified in the designation instrument; and
- includes additional information which constitutes the computation of that designated information in combination with information (including designated information) to make one or both sets of information intelligible; and
- does not include 'value added data' (see section 1.2 below).

Recommendation 2

In conjunction with the proposed principles for the definition of CDR data set out above, Commonwealth Bank proposes that 'value added data' that is excluded from the CDR regime should constitute information which:

- is created through the application of material enhancement, logic, algorithmic processing, or any proprietary process (including any process in which intellectual property rights subsist or other right such as confidential information or trade secrets) to any information (including CDR data); or
- is created through the combination of information (including CDR data) with other information (including CDR data) with the purpose of deriving new information which may be used to make a judgement or base an understanding of any characteristics, behaviour, activities, assets, or property, of a CDR consumer; and
- does not include information which constitutes the computation of information in combination with other information to make the first-mentioned information (or both sets of information) intelligible.

Recommendation 3

Commonwealth Bank recommends that the phrase '*wholly or partly derived*' be used consistently through the legislation in place of '*directly or indirectly derived* and its use be limited to the definition of data holder.

In conjunction with the changes suggested in section 1.3 below, section 56AG(1)(a) should be deleted to avoid confusion in the interpretation of the definition of CDR data.

Recommendation 4

The Bill and designation instrument should specify that product data only includes data that is publicly available, in digital form, and does not include bespoke or tailored offerings.

Recommendation 5:

In order to enhance the benefits of the CDR regime for consumers associated with reciprocal data transfer obligations, the Bill should provide guidance for the transfer of data held by accredited data recipients that may not fall within the current definition of CDR data.

The Bill should reflect the principal 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.

Accreditation of potential data recipients should be contingent upon the identification of equivalent data sets and processes that would allow them to meet reciprocal disclosure obligations. Equivalent datasets should not be limited in definition by what is already captured in the designation instrument but should include 'core consumer data' collected by the accredited entity.

Recommendation 6:

The consumer data rules should clarify the reference to products which involve taking money on deposit and making advances of money such that it captures the products of non-bank lenders.

The definition of "products" should be broadened to include data relating to other kinds of financial products and financial services held by non-ADI's. A further consultation should be undertaken regarding the kinds of products and services offered by non-ADIs and the associated specified classes of information to be designated.

Recommendation 7:

The Bill should provide that the Minister must undertake the same consultation process and consideration of matters in each sub-section of section 56AD before both 'making or amending an instrument under subsection 56AC(2)'.

The amendment of an instrument designating a sector should require the same consultation process and consideration of matters undertaken by the Minister as the making of a new instrument. This will ensure the Minister considers the relevant effects, regulatory impacts and any other relevant matters arising from amendments to an instrument and the likely effect of such amendments to an instrument on the privacy or confidentiality of consumers' information as determined by the Information Commissioner.

Recommendation 8:

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, particularly with respect to the potential technical and financial burden relating to the designation.

Recommendation 9:

Commonwealth Bank recommends that the Bill clarify the application of the Privacy Safeguards where a data holder is acting in its capacity as an accredited data recipient such as exceptions for compliance with some of the Privacy Safeguards for data holders in their capacity as accredited data recipients, due to the regulatory and technical complexity for data holders to comply with the Privacy Act and the Privacy Safeguards regarding CDR data it holds and receives which are stored in the same systems and subject to the same processes.

Recommendation 10:

Commonwealth Bank recommends that Privacy Safeguard 1 be amended to align with APP 1 to allow a CDR participant to make CDR data policies in a form that it considers appropriate, as may be supplemented by guidance from the OAIC or the consumer data rules in a commensurate manner to privacy policies under the Privacy Act.

Recommendation 11:

Exceptions to the consent requirement should be set out in the consumer data rules to address the types of disclosures that occur during the ordinary course of business such as use or disclosure to outsourced service providers and permitted situations where consent would not be required (similar to the framework that currently exists under the Privacy Act).

Recommendation 12:

The CDR regime should impose additional requirements for disclosures to non-accredited data recipients. This could occur:

(a) by establishing under the consumer data rules less stringent tiers of accreditation for lower risk data or classes of participants which act on behalf of the CDR consumer as an extension of that CDR consumer (e.g. where the CDR consumer could download data or print statements and hand them to an accountant). Such an agent

would be required to comply with a minimum security standard and use the CDR data only for the purpose it was provided; and

(b) adopting the principle in the Bill and the Privacy Act used in relation to cross-border disclosures of personal information, which requires APP entities to take reasonable steps to ensure that recipients do not breach the APPs.

Under this model:

- the accredited data recipient would be required to take reasonable steps, including in its terms and conditions, to ensure that non-accredited persons comply with the CDR regime, such as use of the CDR data for the expressed purpose (and not, for example, to on-sell that CDR data or use it for direct marketing where consent has not been provided), protecting the security of CDR data and notification of CDR data breaches;

- a CDR consumer is entitled to complain to OAIC for misuse of data by non-accredited person; and

- the accredited data recipient is liable for the acts or omissions of the third party that contravene the CDR regime, similar to the liability of APP entities for breaches of the Australian Privacy Principles by overseas recipients under section 16C of the Privacy Act.

The liability shield in section 56GC of the Bill should not be available to accredited data recipients that disclose CDR data to non-accredited data recipients to incentivise accredited data recipients to flow down their obligations under the CDR regime to non-accredited data recipients through contractual arrangements.

This approach is largely similar to the intended approach that Treasury is taking with Privacy Safeguard 8, in respect of cross-border transfers of CDR data. As such, a similar model could be applied in respect of disclosures to non-accredited entities.

Recommendation 13:

Amend Privacy Safeguard 7 to accommodate interaction with other legislation such as the *Spam Act (2003)* and *Do Not Call Register Act (2006)*.

Recommendation 14:

Commonwealth Bank recommends deleting section 56EO(1)(b)(ii) so that Privacy Safeguard 13 does not apply to CDR data which is directly or indirectly derived from CDR data.

Recommendation 15:

Accordingly, 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 16:

The Bill should include exemptions from the CDR where a CDR participant is required to comply with foreign laws, particularly where those laws are also intended to protect the privacy of data or relate to financial services regulatory compliance.

Recommendation 17:

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 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

1.1 Derived data and value added data

The updated draft of the Bill includes further detail on how datasets may be included in-scope for the Consumer Data Right (**CDR**) regime and the designation instrument provides more clarity on the specific datasets that may be so included.

The additional provisions are very helpful in demonstrating the Treasury's intent in limiting the scope of value added data that may be subject to the CDR regime. However, as the definition of CDR data has not materially altered in the second exposure draft of the Bill, Commonwealth Bank considers that the definition and its use, including in the additional limitation at section 56BC(3), continues to pose an issue with respect to interpretation of the scope of CDR data.

Sections 56BC(3) and 56BD(2) of the Bill assist with limiting the circumstances in which the consumer data rules made by the ACCC may require the disclosure of derived data by data holders. The intended circumstances are:

- if there is CDR data (*and is not intended to include derived data*) for which there are one or more CDR consumers, then the consumer data rules may not require disclosure of such information unless it is specified in a designation instrument made by the Treasurer under section 56AC(2); and

- where the CDR data (*intending to include derived data*) does not have a CDR consumer, then the consumer data rules can only require disclosure of such information if the CDR data is about the eligibility criteria, terms and conditions, or price of a product or other kind of good, or a service.

Commonwealth Bank supports the principle contained in the limitations; however, the definition of CDR data in section 56AF of the Bill includes information which is designated in the designation instrument *and* information '*that is wholly or partly derived from information*' in section 56AF(a). This appears to create circularity in the use of the definition of CDR data in the Bill.

As currently drafted, CDR data which may be disclosed may be interpreted to include information which is wholly or partly derived (note, not directly or indirectly derived – also see section 1.3 below) from information which is designated. This information could be interpreted to constitute insights, analysis or information which has been transformed by the data holder, circumventing the effect of section 56BC(3). Commonwealth Bank understands that this is not the intent of the Treasury.

Commonwealth Bank considers that amendments to the Bill should be made to address Treasury's intent of ensuring that certain information (being information that is derived from information which is designated) be captured such that the CDR regime:

- includes data that has been enhanced, but not materially so (for example, account balances); and

- regulates the use and disclosure of information derived from information which is designated, through the application of the limitations and definition of data holder.

Recommendation 1

Commonwealth Bank considers that the Treasury can achieve its intent, benefit consumers, and ensure investment certainty and innovation in the data economy by amending the definition of CDR data to capture the principles that CDR data is information:

- that is specified in the designation instrument; and

- includes additional information which constitutes the computation of that designated information in combination with information (including designated information) to make one or both sets of information intelligible; and

- does not include 'value added data' (see section 1.2 below).

1.2 'Value added data'

Consistent with the Open Banking Review, Commonwealth Bank considers that materially enhanced data should not be in-scope of the CDR regime. The Open Banking Review recommended that, as a general rule, '*data that results from material enhancement by the application of insight, analysis or transformation*' should not be included in scope, but that '*there can be exceptions to, or qualification of, this broad principle*'.[1]

The materials accompanying the updated CDR exposure draft make clear that '*The Government's policy is that the scope of information that could be included in the Consumer Data Right is as recommended in the Open Banking Review*'.[2] However increasing clarity within the Bill would underline this intent.

Further, the exclusion of value added data from the possibility of designation is necessary to avoid the unintended consequence of discouraging data-driven innovation and reducing market investment in the same. Following the amendment of section 56AD, the Minister is required to consider 'any intellectual property in the information to be covered by the instrument', which may be used to support such an exclusion; however, Commonwealth Bank considers that this does not provide appropriate assurance to CDR participants.

Recommendation 2

In conjunction with the proposed principles for the definition of CDR data set out above, Commonwealth Bank proposes that 'value added data' that is excluded from the CDR regime should constitute information which:

- is created through the application of material enhancement, logic, algorithmic processing, or any proprietary process (including any process in which intellectual property rights subsist or other right such as confidential information or trade secrets) to any information (including CDR data); or
- is created through the combination of information (including CDR data) with other information (including CDR data) with the purpose of deriving new information which may be used to make a judgement or base an understanding of any characteristics, behaviour, activities, assets, or property, of a CDR consumer; and
- does not include information which constitutes the computation of information in combination with other information to make the first-mentioned information (or both sets of information) intelligible.

1.3 '*Wholly or partly*' or '*directly or indirectly*' derived information

As touched upon above, the circularity in the definition of CDR data and use of the phrases '*wholly or partly derived* and '*directly or indirectly derived* creates uncertainty of interpretation in the Bill. For example, uncertainty is introduced in the definition of a data holder by the repetition of 'CDR data' in both sections 56AG(1) and 56AG(1)(a).

The Bill's explanation of the meaning of '*directly or indirectly derived* from other CDR data appears to refer to a broader set of information than CDR data that is '*wholly or partly derived*, which would mean that a person can qualify as a data holder even if it holds information which would not fall within the definition of CDR data. The reason for such a distinction is unclear.

The use of the phrase *'directly or indirectly derived* is primarily used in the definition of data holder and therefore, if (together with the other proposals in this section 1) the circularity in definition of CDR data is removed and the phrase '*wholly or partly*' is used consistently, a data holder will be a person which holds information:

- which is designated;
- is wholly or partly derived from the designated information; and

[1] Treasury, (December 2017), *The Report of the Review into Open Banking in Australia*, p.38
[2] Treasury, 2018, *Treasury Laws Amendment (Consumer Data Right) Bill 2018: Provisions for further consultation – proposals*, p.4.

- which has not resulted from a process of material enhancement.

This will extend to CDR participants that have not received such information under the consumer data rules, allowing a consumer to request that information in the hands of a non-ADI from whom that consumer receives products or services, and requiring its disclosure to a data holder in its capacity as an accredited data recipient. This will allow the consumer to receive products and services which are better suited to them due to the products and services being based upon a holistic picture of that consumer's behaviour.

Commonwealth Bank considers that, as the definition of CDR data is so fundamental to the operation of the CDR regime, such an approach to the definition of CDR data is important to:

- create consistency and fairness in the CDR regime;
- put the consumer in the centre of data exchanges; and
- encourage innovation, assist with the development of bespoke consumer products, and facilitate responsible lending decisions.

Recommendation 3

Commonwealth Bank recommends that the phrase '*wholly or partly derived*' be used consistently through the legislation in place of '*directly or indirectly derived* and its use be limited to the definition of data holder.

In conjunction with the changes suggested above, section 56AG(1)(a) should be deleted to avoid confusion in the interpretation of the definition of CDR data.

1.4 Product data

The Open Banking review recommended that if data holders are under an existing obligation to disclose information on their products and services, that information should be made publicly available.

Nonetheless, the scope of product data is vaguely defined in the CDR Rules Framework and designation instrument to include 'customer eligibility criteria' and the 'features and benefits' of the product.

Despite the explanatory statement for the designation instrument suggesting that this would relate to 'product information that is public', the broad scope of what product data will include may, for example, inadvertently capture bespoke offerings to large businesses.

Recommendation 4

The Bill and designation instrument should specify that product data only includes data that is publicly available, in digital form, and does not include bespoke or tailored offerings.

2. PRINCIPLES OF RECIPROCITY

2.1 Equivalent datasets for reciprocity

In its publication of 9 May 2018 titled 'Consumer Data Right', the Treasury detailed that the enabling legislation for the CDR would incorporate a principle of reciprocity in circumstances determined by the rules made the ACCC. Commonwealth Bank's previous submission highlighted the benefits provided by including principles of reciprocity in the CDR regime, as identified by Recommendation 3.9 of the Review into Open Banking.

The Consumer Data Right Rules Framework published by the ACCC states that the first version of the rules will not address principles of reciprocity due to the complex issues raised. The legislation should be amended to require the ACCC to make rules to give effect to reciprocity requirements on accredited data recipients.

The Bill should provide the basic framework for reciprocity which may be substantiated by the rules. As currently drafted, the definition of CDR data only encompasses information specified by a designation instrument and any derived data.

The Bill does not make provision for the disclosure of data that is not CDR data and should be amended to require the transfer of 'equivalent' data sets by accredited data recipients, as a condition of becoming accredited. Any obligation to disclose should only arise at the customer's direction.

In order to maximise the value of the CDR regime, the Bill should require that the accreditation of potential data recipients is contingent upon the identification of equivalent data sets and processes that would allow them to meet reciprocal disclosure obligations. The legislation should specify the principles of equivalency to be established in the accreditation process by the ACCC.

These principles should specify that the equivalent dataset should not be defined solely by an existing designation instrument but should identify 'core consumer data' held by that entity. A test should be applied to the entity applying for accreditation: If companies already captured by a designation instrument were to compete with the newly accredited entity, what information of a raw or derived form would allow them to provide a competitive service to its consumers? This test would ensure that any form of data falling into this category would be made available to be shared in a standardised form with other industry participants at the direction of the consumer.

Recommendation 5:

In order to enhance the benefits of the CDR regime for consumers associated with reciprocal data transfer obligations, the Bill should provide guidance for the transfer of data held by accredited data recipients that may not fall within the current definition of CDR data.

The Bill should reflect the principal 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.

Accreditation of potential data recipients should be contingent upon the identification of equivalent data sets and processes that would allow them to meet reciprocal disclosure obligations. Equivalent datasets should not be limited in definition by what is already captured in the designation instrument but should include 'core consumer data' collected by the newly-accredited entity.

2.2 Designated datasets for reciprocity

In addition to implementing the recommendations from the Open Banking Review as discussed above, and in order to execute on the intent of the Treasury's amendments to the definition of data holder within the new framework for reciprocity, the definition of 'product' in the designation instrument should be broadened.

As currently drafted, the definition of 'product', in relation to which information will become subject to the CDR regime, comprises products connected to a banking business, taking money on deposit, making advances of money and other financial activities within the definition of the *Banking Act 1959* (Cth).

This has the effect that the majority of accredited persons from whom exchange of data in reciprocity would have the greatest benefit for consumers will be excluded from the principle of reciprocity on the basis that those accredited persons, for the majority, will not be conducting banking business.

Commonwealth Bank is supportive of the reference to products which involve taking money on deposit and making advances of money and supports clarification in the consumer data rules that such references are intended to capture the products of non-bank lenders.

However, in order to implement a truly effective CDR regime and encourage the development of technologies to allow for efficient and effective transfers of data for which a consumer will request and will benefit, Commonwealth Bank considers that there is room for the definition of "products" to be broadened to include data relating to other kinds of financial products and financial services held by non-ADI's. Commonwealth Bank suggests that a further consultation is undertaken regarding the kinds of products and services offered by non-ADIs and the associated specified classes of information to be designated. A broader definition would enable consumers to benefit from the ability to share consumer data held by data holders which are not ADIs and do not undertake banking activities but which operate in the financial services sector.

Recommendation 6:

The consumer data rules should clarify the reference to products which involve taking money on deposit and making advances of money such that it captures the products of non-bank lenders.

The definition of "products" should be broadened to include data relating to other kinds of financial products and financial services held by non-ADI's. A further consultation should be undertaken regarding the kinds of products and services offered by non-ADIs and the associated specified classes of information to be designated.

3. REGULATORY POWERS

3.1 Consultation

The amendment of an instrument designating a sector should require the same consultation process and consideration of matters undertaken by the Minister as the making of a new instrument. This will ensure the Minister considers the relevant effects, regulatory impacts and any other relevant matters arising from amendments to an instrument and the likely effect of such amendments to an instrument on the privacy or confidentiality of consumers' information as determined by the Information Commissioner.

The Bill remains silent on whether the Minister can amend an 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. 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, Commonwealth Bank proposes that the Bill expressly set out that any amendments to the instrument of designation be subject to the same consultation process and consideration of matters required for the making of an instrument currently set out in section 56AD of the Bill.

Recommendation 7:

The Bill should provide that the Minister must undertake the same consultation process and consideration of matters in each sub-section of section 56AD before both 'making or amending an instrument under subsection 56A(2)'.

The amendment of an instrument designating a sector should require the same consultation process and consideration of matters undertaken by the Minister as the making of a new instrument. This will ensure the Minister considers the relevant effects, regulatory impacts and any other relevant matters arising from amendments to an instrument and the likely effect of such amendments to an instrument on the privacy or confidentiality of consumers' information as determined by the Information Commissioner.

3.2 Process for designating datasets

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.

Recommendation 8:

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, particularly with respect to the potential technical and financial burden relating to the designation.

4. CDR PRIVACY SAFEGUARDS

4.1 Clarifying the interaction of the Privacy Safeguards with the Privacy Act

Commonwealth Bank supports the changes made to the Privacy Safeguards, clarifying the operation of the Australian Privacy Principles and the Privacy Safeguards for data holders, accredited data recipients and accredited persons.

However, we note that there remain some matters raised by Commonwealth Bank's previous submissions which have not been addressed, or which raise new issues as a result of the changes made in the second exposure draft Bill. As such, Commonwealth Bank believes that the changes made to the Privacy Safeguards have unintended consequences for data holders that are holding CDR data in their capacity as accredited data recipients.

While Commonwealth Bank appreciates that the consumer data rules are intended to determine when the Privacy Safeguards do / do not apply to a data holder and data sets which are ingested (determined on the basis of whether the CDR data being ingested is / is not data which the data holder ordinarily holds), we consider that this should be clarified in the Bill and guidance be provided in the consumer data rules.

For example, while sections 1.42 – 1.44 of the Explanatory Materials state that the Privacy Safeguards will apply differently to a data holder in its capacity as an accredited data recipient, section 56AG(4), sections 56EC(4) and (5), and the Privacy Safeguards do not appear to clearly achieve the intent of the Treasury in '*changing the privacy protections applying to the CDR data so that the APPs, as applicable, apply to a data holder's ongoing use of that CDR data*'.[3]

The complexity primarily arises from:

- the process of combination of data sets in the ordinary course of business for the provision of products or services to a consumer and the technical capability required to segregate and treat different components of a customer record in accordance with distinct regimes; and

- the practical reality that, although the APPs may be substituted for the Privacy Safeguards for accredited data recipients, any such data will be housed in the same systems and databases irrespective of the capacity in which the data was received.

Solving for this complexity has potential to create significant financial and technical burdens for data holders, for example to apply methods of tagging different parts of the same customer record to comply with the APPs or the Privacy Safeguards and discriminating whether any such parts are data which the data holder does, or does not, ordinarily hold as determined by the consumer data rules.

Set out below are a number of Privacy Safeguards which Commonwealth Bank considers do not clearly achieve the Treasury's intent and, on the basis of the background above, may pose a problem for CDR participants if not adequately addressed and clarified in the Bill.

4.2 Clarifying the application of the Privacy Safeguards to CDR participants

There is complexity for data holders such as Commonwealth Bank, that are already subject to the Australian Privacy Principles to the extent that any CDR data they are holding is personal information, arising from additional and potentially inconsistent obligations under some of the Privacy Safeguards in their capacity as accredited data recipients. For example, Privacy Safeguard 8 (Cross-border disclosure) will apply to restrict an accredited data recipient from disclosing CDR data outside Australia unless the new recipient is an accredited person or permitted under the consumer data rules.

Similarly, the requirement under Privacy Safeguard 12 (Security) for an accredited data recipient to destroy or de-identify CDR data that it no longer needs for the purposes under the consumer data rules may not be practical for data holders to comply with in their capacity as accredited data recipients. A consequence of this Privacy Safeguard 12 would be that data holders would need to carefully distinguish between CDR data it holds as a data holder and as an accredited data recipient then apply either APP 11 (Security) (if the data is personal information) or Privacy Safeguard 12 to that CDR data, when in practice, such CDR datasets would comprise a whole customer record.

Recommendation 9:

[3] Treasury Laws Amendment (Consumer Data Right) Bill 2018: Provisions for Further Consultation Explanatory Materials p.8.

Commonwealth Bank recommends that the Bill clarify the application of the Privacy Safeguards where a data holder is acting in its capacity as an accredited data recipient such as exceptions for compliance with some of the Privacy Safeguards for data holders in their capacity as accredited data recipients, due to the regulatory and technical complexity for data holders to comply with the Privacy Act and the Privacy Safeguards regarding CDR data it holds and receives which are stored in the same systems and subject to the same processes.

4.3 Privacy Safeguard 1 – Open and Transparent Management of CDR Data

The second exposure draft of the Bill includes a requirement for CDR data policies to be 'in a form approved in accordance with the consumer data rules'.

Commonwealth Bank queries whether this is a necessary inclusion, given that a privacy policy under Australian Privacy Principle 1 (**APP 1**) does not have a mandated form. Commonwealth Bank is not aware of concerns across the banking industry or other sectors of the economy regarding the format of privacy policies, despite the absence of a requirement for a mandated or approved form.

Given the significant overlap in respect of the practices that will apply to how a business uses, handles and otherwise managed information, it is possible that data holders and accredited data recipients will prepare an updated privacy policy that includes the relevant requirements for this document to also meet the requirements of a CDR policy. This would be similar to the commonly-used practice of including a credit reporting policy (required under section 21B of the Privacy Act) in the same document as the organisation's privacy policy.

Creation of multiple policies may cause consumer uncertainty as to the rights the consumer may have, particularly where those consumers are unaware which regime may apply to their data or information.

Recommendation 10:

Commonwealth Bank recommends that Privacy Safeguard 1 be amended to align with APP 1 to allow a CDR participant to make CDR data policies in a form that it considers appropriate, as may be supplemented by guidance from the OAIC or the consumer data rules in a commensurate manner to privacy policies under the Privacy Act.

4.4 Privacy Safeguard 6 – Use or Disclosure of CDR Data

4.4.1 Consent requirements

As touched upon above, in Commonwealth Bank's view, the amended form of this Privacy Safeguard in particular may lead to issues with use and disclosure rights of CDR Data in the ordinary course of business, given that essentially all uses and disclosures require consent from the CDR consumer.

While Commonwealth Bank respects the principle of ensuring consent is obtained for use and disclosure of CDR data, there are certain situations where it may be impractical to obtain consent for CDR data to be disclosed to outsourced service providers and it may be preferable for the consumer to rely upon information regarding outsourcing arrangements contained in a CDR policy rather than providing express consent. For example, use or disclosure to outsourced service providers (such as cloud service providers) may occur on an ongoing basis and the requirements to seek consent for every use or disclosure may result in unwieldy consents or mean that the consent requirements are not met.

Further, the requirement of consent makes it more difficult for the consumer data rules to set out general circumstances where disclosure may be permitted without prior consent (such as the 'permitted general situation' or 'permitted health situations' concepts that exist under the Privacy Act). While these may only arise under limited circumstances, obtaining consent to these uses or disclosures will often be impractical and contrary to the public interest.

Commonwealth Bank proposes that whether a particular use or disclosure requires consent could be dealt with in the consumer data rules or be subject to additional requirements.

Recommendation 11:

Exceptions to the consent requirement should be set out in the consumer data rules to address the types of disclosures that occur during the ordinary course of business such as use or disclosure to outsourced service providers and permitted situations where consent would not be required (similar to the framework that currently exists under the Privacy Act).

Supplementing the above:

- the accreditation framework should address the technical and organisational measures which an accredited data recipient must implement to address security (including the security of its suppliers and their subcontractors); and

- similar to standards such as ASIC's RG 104 and APRA's CPS231, the consumer data rules should include obligations on accredited data recipients with respect to contractual protections which are required when engaging service providers for the provision of services which involve the disclosure and use of CDR data, including with respect to use (e.g. only for the purposes of providing services to the accredited data recipient), disclosure (e.g. to approved subcontractors), accuracy, storage, deletion and security.

4.4.2 Restrictions on non-accredited data recipients

Under the ACCC's current draft of the CDR Rules Framework, we note that the ACCC appears to have taken the view that there may be free disclosure of CDR data to non-accredited persons for the purpose of that non-accredited person's use (as distinct from arrangements where that non-accredited person provides services to an accredited data recipient), provided that consent has been given.

In light of this, and as an alternative to the restrictions on the scope of the consumer data rules set out in the second exposure draft Bill, Commonwealth Bank recommends that more stringent requirements are included in the Bill to ensure that CDR data disclosed under the CDR regime continues to be protected in all circumstances.

Commonwealth Bank is conscious that the provision of CDR data to non-accredited persons could compromise the integrity and security of the CDR regime, because those persons are not required to comply with the CDR regime.

Where there is scope for CDR data to be provided to non-accredited parties by consent of the CDR consumer, this may be exploited by those entities. For example, the non-accredited entity may use CDR data collected from clients for aggregation and use that for purposes other than the purposes the CDR data was originally provided, such as to create and sell databases for direct marketing.

Risks associated with this has concept have been somewhat addressed through the inclusion of the 'new recipient' concept in Privacy Safeguard 8, which requires that the disclosure not be made unless 'the conditions specified in the consumer data rules are met', as well as the restrictions on rule-making set out in section 56BC(1) and (3) of the Bill. However, the Privacy Safeguard 8 requirement only applies to cross-border disclosure and the restrictions in section 56BC may not be sufficient where disclosure to a non-accredited person is required.

In addition, the proposed new restrictions on disclosure under the consumer data rules in section 56BG(3) are not relevant to this point, as that provision only applies to limit the CDR data which may be required to be disclosed, as opposed to permitted CDR data to be disclosed.

Recommendation 12:

The CDR regime should impose additional requirements for disclosures to non-accredited data recipients. This could occur:

(a) by establishing under the consumer data rules a second or less stringent tier of accreditation for a class of participants which act on behalf of the CDR consumer as an extension of that CDR consumer (e.g. where the CDR consumer could download data or print statements and hand them to an accountant). Such an agent would be required to comply with a minimum security standard and use the CDR data only for the purpose it was provided; and

(b) adopting the principle in the Bill and the Privacy Act used in relation to cross-border disclosures of personal information, which requires APP entities to take reasonable steps to ensure that recipients do not breach the APPs.

Under this model:

- the accredited data recipient would be required to take reasonable steps, including in its terms and conditions, to ensure that non-accredited persons comply with the CDR regime, such as use of the CDR data for the expressed purpose (and not, for example, to on-sell that CDR data or use it for direct marketing where consent has not been provided), protecting the security of CDR data and notification of CDR data breaches;

- a CDR consumer is entitled to complain to OAIC for misuse of data by non-accredited person; and

- the accredited data recipient is liable for the acts or omissions of the third party that contravene the CDR regime, similar to the liability of APP entities for breaches of the Australian Privacy Principles by overseas recipients under section 16C of the Privacy Act.

The liability shield in section 56GC of the Bill should not be available to accredited data recipients that disclose CDR data to non-accredited data recipients to incentivise accredited data recipients to flow down their obligations under the CDR regime to non-accredited data recipients through contractual arrangements.

This approach is largely similar to the intended approach that Treasury is taking with Privacy Safeguard 8, in respect of cross-border transfers of CDR data. As such, a similar model could be applied in respect of disclosures to non-accredited entities.

4.5 Privacy Safeguard 7 – Direct Marketing

In Commonwealth Bank's previous submission, we noted that 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)*. This has not been addressed in the updated drafting to Privacy Safeguard 7.

Recommendation 13:

Amend Privacy Safeguard 7 to accommodate interaction with other legislation such as the *Spam Act (2003)* and *Do Not Call Register Act (2006)*.

4.6 Privacy Safeguard 13 – Correction of CDR data

Commonwealth Bank is concerned with the application of Privacy Safeguard 13 to CDR data which has been directly or indirectly derived from CDR data. In some circumstances, where information has been de-identified or aggregated, it may be difficult if not impossible for a data holder to identify which parts of the CDR data relate to the CDR consumer, and then to correct the data or to include a statement which verifies that the CDR data is accurate, up to date, complete and not misleading in relation to the CDR consumer.

Recommendation 14:

Commonwealth Bank recommends deleting section 56EO(1)(b)(ii) so that Privacy Safeguard 13 does not apply to CDR data which is directly or indirectly derived from CDR data.

5. CONSISTENCY WITH OTHER REGULATORY REGIMES

5.1 Relationship with other laws

Although the relationship between the Privacy Safeguards and the APPs has been given some consideration, Commonwealth Bank considers that the updated exposure draft Bill does not sufficiently address the relationship between the Bill and other laws (including foreign laws).

These are discussed further this in this section. As a general proposition, it is Commonwealth Bank's view that the regulatory obligations of CDR participants should take precedence over the Privacy Safeguards.

5.2 Interaction with the Privacy Act and CCR Bill

Although the updated version of the Bill incorporates amendments to separate the obligations under the APPs and the Privacy Safeguards, there are other issues of potential regulatory interactions that have not been resolved. As addressed in section 7.1 of our previous submission, these include Part IIIA of the Privacy Act and the *National Consumer Credit Protection Amendment (Mandatory Comprehensive Credit Reporting) Bill 2018* (**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.

Recommendation 15:

Accordingly, 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.

5.3 International obligations

The second exposure draft of the Bill does not address how it will interact with obligations that CDR participants may have under foreign laws, such as the European Union's General Data Protection Regulation (**GDPR**) or the Markets in Financial Instruments Directive (**MIFID II**).

For some Australian banks, including Commonwealth Bank, certain information held in relation to customers falls within the scope of personal data regulated under the GDPR, as a result of the bank's activities in the region. Depending on the final scope of the designation instrument, it is likely that the GDPR may apply to CDR data, which creates the potential for conflicting obligations to apply to Commonwealth Bank and other CDR participants. For example, under the GDPR consumers are granted a right of 'data portability' (Article 20 – Right to Data Portability) which allows for the automated transfer of personal data from one data controller to another, similar to the CDR regime. Where this right applies to an accredited data recipient and a request is made under the GDPR in relation to certain CDR data, there is the potential for these obligations to conflict with the CDR regime and the Privacy Safeguards.

Commonwealth Bank is also concerned that the Privacy Safeguards do not provide it with the flexibility to comply with the retention requirements under MIFID II. The obligations in Privacy Safeguard 12 require deletion of CDR data where the data is not needed for the purposes permitted under the consumer data rules or for the purpose for which an accredited data recipient is permitted to use or disclose CDR data. While there is an exception to comply with Australian law, there is no equivalent exception that permits CDR recipients who have retention obligations under foreign laws (such as MIFID II) to retain that information.

Commonwealth Bank believes that there should be exemptions from the CDR where a CDR participant is required to comply with foreign laws, particular where those laws address the use, disclosure, retention, privacy or security of data that may fall within the scope of CDR data.

This is to ensure that CDR participants are able to comply with their various regulatory obligations. As with other regulatory conflicts, Commonwealth Bank does not believe it is appropriate for these issues to be left to the consumer data rules to be resolved.

It is recommended that the Privacy Safeguards are updated to include an exemption from compliance where a foreign law or court order requires different treatment of that data outside of Australia. This exemption may be similar to the exemption in section 13D of the Privacy Act, which provides that an act or practice done or engaged in outside Australia does not give rise

to an 'interference with the privacy of an individual' if the act or practice is required by an applicable law of a foreign country.

Recommendation 16:

The Bill should include exemptions from the CDR where a CDR participant is required to comply with foreign laws, particular where those laws are also intended to protect the privacy of data or relate to financial services regulatory compliance.

6. LIABILITY AND ENFORCEMENT

6.1 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 regime 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);
- **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.

6.2 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 17:

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 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.