12 October 2018

Consumer Data Right Division
Australian Competition and Consumer Commission
23 Marcus Clarke Street,
Canberra ACT 2601

Via email: ACCC-CDR@accc.gov.au

Commonwealth Bank welcomes the opportunity to respond to the Australian Competition and Consumer Commission's draft Consumer Data Right (**CDR**) Rules Framework (the **Rules**) and the ACCC's ongoing engagement with industry.

The CDR is a reform that has the potential to drive significant economic benefits for consumers for decades to come. As one of the first organisations to be delivering the CDR for our customers, Commonwealth Bank is committed to building trust in the regime and maximising its benefit for all Australians.

The Government has announced ambitious targets for the implementation of the CDR regime.

In meeting these targets, industry should prioritise three key principles. The first is to focus on areas where participants can deliver the greatest benefit to the greatest number of consumers. The ACCC has identified a number of complex problems, requiring significant industry consultation, where only small numbers of consumers will see a benefit in the initial stages of the regime. Commonwealth Bank considers that these issues should be carved out from the initial implementation and solved within a reasonable timeframe of the commencement of the regime.

Secondly, there are a number of rules which relate to historical data that are not consistent with the policy principles of the CDR. While it will still be possible to provide access to this data outside of the CDR framework, data holders should focus on the collection, storage and provision of data within the CDR framework on a forward-looking basis. Data included in-scope for the regime should be currently accessible and available in digital form.

And finally, there may be areas of additional complexity, such as introducing an 'intermediary model' into the regime, which require additional industry cooperation to solve for important issues such as capturing informed consent and maintaining rigorous cyber security protections. These problems should be solved in the medium term rather than the initial implementation.

While the ambitious timeframes for the banking sector presents challenges (and means that many work streams will need to be undertaken in parallel), Commonwealth Bank strongly supports a cost-benefit analysis being conducted as part of the Regulatory Impact Statement for the sector. The ACCC is well placed as a regulator to assist with this analysis, and ensure that it informs the ongoing implementation of the CDR regime, through the Rules.

Summary of Recommendations

Recommendation 1:

Former customers should not be brought into scope for the CDR regime until at least two years of the regime commencing.

Data relating to accounts closed before 1 January 2017 should not be included in scope for the CDR regime.

Where customer data has to be provided in a standardised, digital form to both former and existing customers, that data should be limited to two years of transaction history. Where data holders are required to hold customer data for longer periods for legal or regulatory reasons (some customer records will be stored for a period of seven years), this data could be made available to customers via alternative methods.

Recommendation 2:

Commonwealth Bank is supportive in-principle of the inclusion of offline consumers in the CDR regime. However, further consideration should be given to the most appropriate methods to enable data access and sharing for these consumers, including the appropriateness of existing channels. Commonwealth Bank proposes two solutions for how offline consumers should be included in the CDR regime:

a. the first approach is to create an on-boarding experience for offline consumers to establish a digital channel and provide assistance (e.g. physically in branches) in relation to accessing and sharing their CDR data; or
b. a second approach is to establish an industry working group with the purpose of considering the appropriateness of designing an alternative access method for offline consumers, and the rules and standards that would be required to support such an alternative model.

Recommendation 3:

The Rules should reinforce the principle, to be captured in the Bill, that 'value-added data' is out of scope of the CDR regime and constitutes information which:

a. 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
b. 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
c. 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 4:

Where balances and other fields are derived from raw data, there are technical constraints on how often this data is refreshed. To ensure that the provided data is accurate and usable, the requirements to make data available in the CDR regime should align with the cadence that this data would normally be processed by the data holder. For instance, if a balance on a credit product is calculated daily, then that balance should not be required to be provided more frequently than daily under the CDR regime.

Additionally, the data-fields should be reviewed for specific privacy concerns, including the identification of third parties via sensitive banking information (including BSB numbers and account details).

As noted above, data included in bank statements that does not directly relate to specific transactions, such as direct marketing messages, should not be included in-scope for the CDR regime.

Recommendation 5:

Commonwealth Bank recommends that metadata be excluded from the scope of transaction data under the Rules.

Recommendation 6:

Customer-level data that is not currently collected and held in a standard manner throughout the industry should not be included in the CDR regime at its commencement.

Where customer-level data constitutes value-added data, this should be excluded from the scope of the CDR regime.

Products for which product information is not currently available in a digitally-accessible form should not be included in the scope of the CDR regime.

Recommendation 7:

The ACCC should introduce an equivalence test as part of the accreditation process, to be applied to any entity applying to become an accredited data recipient under the CDR framework. The ACCC should not be bound by the data listed in the existing designation instrument with respect to reciprocity but should instead enquire about the types of core data necessary to the provision of a service. Any accredited data recipient (subject to the limited exception in Recommendation 8) should make their core customer data available to be shared under the Rules at the consumer's request.

Recommendation 8:

A general exemption to reciprocity requirements should be granted to small businesses (including all related bodies corporate). Such thresholds should be aligned with accepted definitions of 'small business', such as those in the Code of Banking Practice.

Recommendation 9:

The Rules should include a 'reasonable steps' provision to allow the withholding of data by a data holder in the event that an accredited data recipient to whom the data holder would transfer data is found to have not taken reasonable steps to protect consumer data.

Additionally, an annual attestation for accredited data recipients should be built into the accreditation process to ensure compliance with industry best practice cyber security standards.

Recommendation 10:

Commonwealth Bank has identified a number of complex authorisation structures which should be carved out of the Rules. Commonwealth Bank considers that these types of authorisation structures should not be brought within scope of the CDR regime at the commencement of the regime. These authorisation structures include:

a. complex personal accounts (e.g. deceased estates); and
b. individuals acting on behalf of consumers, such as authorised signatories.

Recommendation 11:

Commonwealth Bank recommends that the ACCC adopt a phased approach to implementing business accounts focused on simple businesses first.

Complex business entities (e.g. large companies and associations) and multi-entity corporate structures (e.g. partnerships, trusts, JVs, SMSFs) should not be included in the CDR regime at its commencement. The ACCC should only include rules for the inclusion of these entities, after thorough consideration of issues including: appropriate controls for the sharing of sensitive commercial data; managing complex consent structures; and the protection of intellectual property.

Recommendation 12:

Children and minors should not be included in the definition of CDR consumer.

Recommendation 13:

Consent for uses of CDR data should be unbundled so that each specific consent to a use or disclosure needs to be independent of:

a. any other use or disclosure; and
b. any other condition, such as a product purchase.

Recommendation 14:

Commonwealth Bank recommends that the ACCC does not make rules prohibiting data holders from requesting additional information beyond what is described in the rules or standards.

Recommendation 15:

Data holders should not be required to allow consumers to access CDR data via an open API as this would lower security standards, may lead to negative customer outcomes such as additional third parties requesting access to the APIs, and would involve a significant IT build requirement.

Recommendation 16:

Given the complexity of issues surrounding the inclusion of intermediaries into the CDR regime, intermediaries should not be included in the regime for the first 24 months of operation. Industry should use this time to work to solve problems around data collection, use and on-sharing, consent models, accreditation tiers and information security standards.

Recommendation 17:

The ACCC should make rules that include:

a. an accreditation framework which sets the technical and organisational measures which an accredited data recipient must implement to address security (including with respect to its employees and the security of its suppliers and their subcontractors); and
b. standards no lower than ASIC's RG 104 and APRA's CPS231, and similar guidances, and apply those 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.

Recommendation 18:

Foreign entities seeking accreditation under the CDR regime should be required to register under the *Corporations Act 2001* and to be required to provide security for performance such as a bank guarantee or performance bond.

Further, an aggrieved party should have recourse for any claim it has against the accredited data recipient through either the local agent or the principal.

Contents

1 In-scope customers

1.1 Former customers

Commonwealth Bank supports the ACCC's proposal to exclude former customers for the initial phase of the CDR in order to address technical and legal complexities with enabling data sharing on closed accounts. This exclusion should apply to all closed accounts, including those held by current customers.

Limitations and timeline

Accessing data for closed accounts presents technical and legal limitations, particularly with regard to data storage and management. In Commonwealth Bank's view, there are four major limitations to the inclusion of former customers:

a. Many data holders have different methods for storing data across product types, and across time, which includes both digital storage and warehousing. Making historical data available in standardised digital form and in real time or within a short timeframe for former customers would involve a significant investment of time and resources. It is not clear how many customers would benefit from this provision.
b. Personal information collected prior to the introduction of the CDR regime is subject to the Privacy Act. Under the Privacy Act, if an APP entity no longer needs personal information for any purpose for which the information may be used or disclosed, the APP entity is under an obligation to take reasonable steps to destroy or de-identify the data (see Australian Privacy Principle 11). This would necessarily mean that such data would not be available for disclosure under the CDR regime. As such, the right to access data under the CDR regime should not conflict with existing obligations with respect to document retention.
c. To minimise fraud and other risks, former customers will require Know Your Customer (KYC) re-verification so they can be provided access to online banking. Customer relationships may also be terminated by the data holder, such as banks, for contravention of laws or bank policies. Additional consideration should be given to this category of customer, and how flexibility should be granted to data holders to manage their compliance with laws, such as anti-money laundering and counter-terror financing regulations.
d. For some categories of customers (such as business customers with complex authorisation structures), the authority to access data is no longer valid as soon as they terminate a relationship with the data holder (i.e., when an account is closed). This would require an additional build requirement to allow customers to re-establish an account authority.

Recommendation 1:

Former customers should not be brought into scope for the CDR regime until at least two years of the regime commencing.

Data relating to accounts closed before 1 January 2017 should not be included in scope for the CDR regime.

Where customer data has to be provided in a standardised, digital form to both former and existing customers, that data should be limited to two years of transaction history. Where data holders are required to hold customer data for longer periods for legal or regulatory reasons (some customer records will be stored for a period of seven years), this data could be made available to customers via alternative methods.

1.2 Offline consumers

Commonwealth Bank supports the ACCC's proposal to exclude offline consumers from the initial implementation of the CDR regime in order to more fully consider their access needs and requirements.

Limitations and timeline

Commonwealth Bank supports the ACCC's recommendation to consider how consumers who do not use online banking can be brought into the CDR regime. As the ACCC recognises, the Open Banking Review and the CDR regime largely assume access to and sharing of data by digital means, and further consideration will be required to determine the appropriate methods by which consumers without online banking can access the CDR.

One of the ways in which offline consumers can be brought into the regime early is to provide an on-boarding experience through assisted channels, such as bank branches, for customers who wish to access their data online. By providing eligible offline consumers with access to online banking and supported on-boarding, they will be able to access the benefits of the CDR regime as intended.

There are a number of ways that offline consumers could gain access to the CDR without creating an online account, however, further consideration should be given to the useability of alternative models and the extent to which existing channels available to these consumers may enable data access and sharing.

There are a number of features of the existing regime which would require significant re-working to accommodate CDR obligations. For example, new models of consent and authentication may need to be developed to enable data sharing in an offline context. Additionally, providing access to the equivalent of a consent dashboard is problematic outside of existing digital channels, and would again take time to develop among industry participants. Commonwealth Bank would be concerned if customers were able to share data without having access to a dashboard to understand and manage consents on an ongoing basis.

Recommendation 2:

Commonwealth Bank is supportive in-principle of the inclusion of offline consumers in the CDR regime. However, further consideration should be given to the most appropriate methods to enable data access and sharing for these consumers, including the appropriateness of existing channels. Commonwealth Bank proposes two solutions for how offline consumers should be included in the regime:

a. the first approach is to create an on-boarding experience for offline consumers to establish a digital channel and provide assistance (e.g. physically in branches) in relation to accessing and sharing their CDR data; and
b. a second approach is to establish an industry working group with the purpose of considering the appropriateness of designing an alternative access method for offline consumers, and the rules and standards that would be required to support such an alternative model.

2 In-scope data sets

2.1 Derived data

Commonwealth Bank strongly supports the ACCC distinguishing between 'derived data' and 'value-added' data in interpreting the designation instrument under section 56AC(2) of the legislation.

Under this distinction, derived data would include information computed from raw data, whereas value-added data resulting from the 'material enhancement by the application of insights, analysis or transformation by the data holder' would be out of scope of the CDR regime.

If value-added data were to be included within the scope of derived data, data holders would be forced to transfer intellectual property rights to third parties without the protections data holders would customarily expect to be associated with such transfers. For example, typical commercial transfers of such value-added data are generally accompanied by contractual arrangements addressing confidentiality, ownership of intellectual property rights and restrictions on use.

Without adequate protection of their intellectual property rights in data processing methods, data holders will have no incentives to invest in unique and innovative data analysis or enter into commercial partnerships with the innovative providers of these services, which will necessarily reduce the level of new services and products available to customers. This will result in a stifling of innovation, which undermines the objectives of the CDR regime.

Additionally, Commonwealth Bank recognises that the insertion of sections 56BC(3) and 56BD(2) in the updated CDR exposure draft assists with limiting the circumstances in which the Rules made by the ACCC can require the disclosure of derived data by data holders. However, Commonwealth Bank does not consider that these limitations achieve the expressed intent and have made separate submissions with respect to this topic as expressed in the Bill.[1]

Recommendation 3:

The Rules should reinforce the principle, to be captured in the Bill, that 'value-added data' is out of scope of the CDR regime and constitutes information which:

a. 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
b. 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

[1] Treasury Laws Amendment (Consumer Data Right) Bill 2018: Provisions for further consultation.

c. 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.

2.2 Datasets

Commonwealth Bank is broadly supportive of the approach to rule-making on customer data, noting that there will be some overlap by the work being done by Data61 in setting standards around these datasets. We also note that the ACCC's approach to defining in-scope data may change in light of the updated CDR exposure draft.

2.2.1 Customer data

Commonwealth Bank is supportive of providing access to customer data in a form and type that appropriately protects the privacy and security of all account holders. The ACCC appears to suggest that all information that has been provided by the customer may be contemplated, with the ACCC making rules which specify which customer data will be included. Commonwealth Bank seeks the clarification that customer data must be limited appropriately to only designated datasets.

Limitations and timeline

The ACCC contemplates the personal details of consumers being shared in a number of ways including customer contacts details, account contact details, and payee lists. Where customer- or account-level contact details are being shared, Commonwealth Bank considers it should never be permissible for a third party to share the personal details of another party to that same account. For example, if the contact details for a joint savings account are listed for customer A, the other account holder (customer B) should not be permitted under the CDR to require the disclosure of customer A's contact details.

Personal information is frequently used to commit Identity Take-Over in order to compromise customer's accounts and commit fraud. Data holders rely on customer information to verify the identity of customers, and also often rely on the customer being in possession of their mobile phone or a provided email address as a second factor to verify their identity. These high risk data elements should not be shared under the CDR regime.

If this data is provided as part of a data sharing arrangement and the data recipient suffers a data breach, provision of this information is likely to lead to an increase in fraudulent events impacting the customers of data holders and trust in the CDR regime generally. In particular, mobile numbers could be used to commit an account takeover via porting, which is a significant driver of fraud.

There are also technical limitations associated with certain customer data which the ACCC has outlined in the draft Rules. The definition of 'scheduled payments' should be refined to include only recurring payments which are made within the bank's existing digital assets. A broad definition which included, for instance, information about direct debit authorisations, should not be included in scope as banks do not have full visibility of this data, which is established between the customer and merchant.

Further consideration should be given to the privacy and security considerations of sharing payee details, which commonly include name, BSB and account number. In addition, market innovations, such as PayID numbers and external accounting software which stores payee lists externally, mean that banks will not always be able to provide access to payee lists.

Additional information captured as part of a 'payee list' may include personal information of third parties including details of their financial instruments. In line with industry practice, Commonwealth Bank recommends that data that may be sensitive to third parties be obfuscated or tokenized as part of the security practices being defined by Data61.

The requirement to share 'authorisations' should be not be dealt with in the first version of the Rules. There are several technical limitations and privacy concerns. Many accounts (e.g. business accounts and personal accounts that haven't been updated recently) use a paper-based account authority document where signatory names are not accessible digitally. In addition, certain complex customer types have authorities recorded against an online banking 'service' rather than against an account. It would be highly complex to extract service-level authorisations and map those against individual accounts.

2.2.2 Transaction data

Limitations and timeline

There are limitations in the transaction data identified by the ACCC.

Firstly, the transaction descriptions should only be based on what is available in the form of raw data. Any identifiers or categorisation that are the result of enrichment or transformation by the data holder are 'value-added' and should not be in scope. An example of this would include transaction categorisation, where the raw data of the transaction has been transformed into separate spending categories, such as 'health' or 'travel'.

Clarity is required on the permissibility of sharing descriptions (whether populated by the data holder or the customer) where those descriptions include personal information, such as BSB and account numbers. In some cases, there may be additional security requirements on the data required to be shared.

Finally, making all readily available information on a consumer's bank statement in-scope for the CDR is problematic. In some instances, that data will include fields that do not directly relate to transaction history and are derived from raw data (for instance, updates on award points and messages around compliance) and in some cases will contradict the principles of the CDR regime (for instance, the inclusion of direct marketing messages).

Recommendation 4:

Where balances and other fields are derived from raw data, there are technical constraints on how often this data is refreshed. To ensure that the provided data is accurate and usable, the requirements to make data available in the CDR regime should align with the cadence that this data would normally

be processed by the data holder. For instance, if a balance on a credit product is calculated daily, then that balance should not be required to be provided more frequently than daily under the CDR regime.

Additionally, the data-fields should be reviewed for specific privacy concerns, including the identification of third parties via sensitive banking information (including BSB numbers and account details).

As noted above, data included in bank statements that does not directly relate to specific transactions, such as direct marketing messages, should not be included in-scope for the CDR.

2.2.3 Metadata

Limitations and timeline

Commonwealth Bank considers that metadata should not be included in the CDR without careful consideration and consultation.

Firstly, the requirement to share data that is not needed or useful for consumers contradicts data security principles (as enshrined in the Australian Privacy Principles), in that entities should not collect or store more information than is necessary for the provision of services to a consumer. Doing so materially increases the risk of a cyber security breach and puts consumers at risk. While these risks in relation to the sharing of metadata are readily quantifiable (and are significant), the potential use cases are not clear at present. Although any such benefits may become more obvious over time, Commonwealth Bank does not support the inclusion of metadata in the CDR regime at its commencement due to the known high levels of risk and potential to undermine trust in the CDR regime.

Secondly, Commonwealth Bank considers that while metadata may be collected, is not stored (or 'held') in most instances. The underlying principle of the CDR regime is that only data that is currently collected and held by data holders should be in-scope. In many instances, where metadata is not held providing access for customers would involve a material investment. Aggregating and processing metadata about a transaction so that it is in a standardised form capable of being understood by an authorised data recipient will come at a significant cost to data holders. Such costs are difficult to justify where there is no clear benefit to the consumer associated with the transfer of metadata about a transaction.

Recommendation 5:

Commonwealth Bank recommends that metadata be excluded from the scope of CDR data under the Rules.

2.2.4 Product Data

Limitations and timeline

For some products, the calculation of fees and other charges are based on consumer behaviour, rather than product attributes. Such information may be calculated and generated on an ongoing basis, such as at the end of each billing cycle. Including this information in the product data required to be shared under the CDR regime would require standardisation of how industry would report such rates, and there would need to be a flexible cadence for how it would be reported.

Customer-level account information was not included in the recommendations of the Final Report of the Review into Open Banking and the inclusion of this data adds technical complexity to the initial IT build required to give effect to the CDR regime.

In addition, one of the underlying principles of the CDR regime is that the product data in-scope for the CDR regime should be that which is currently accessible and publicly available in digital form. There may be some bespoke products, or products which are no longer sold but are grandfathered to existing customers, where this information will not fit this description and such product data scope should not be included in the CDR regime.

Recommendation 6:

Customer-level product data that is not currently collected and held in a standard manner throughout the industry should not be included in the CDR regime at its commencement.

Where customer-level product data relates to value-added data, this should be excluded from the scope of the CDR regime.

Products for which product information is not currently available in a digitally-accessible form should not be included in the scope of the CDR regime

3 Reciprocity

The principle of reciprocity is fundamental to the CDR regime's ability to promote innovation, and to maximise the benefits of the regime to consumers. Limiting the CDR regime such that it only enables consumers to require their data be shared from data holders to accredited data recipients (but not similarly requiring data recipients to send data the other way, at a customer's request) will considerably lessen the power of consumers to use their data to choose the products that best meet their financial needs. It will also create 'data lakes', where valuable consumer data is monopolised by a small number of large, multinational companies. The outcome over time would see significant information asymmetries, creating an uneven playing field which stifles competition and innovation.

Trying to retrofit a principle of reciprocity after the CDR regime has commenced would be difficult and unnecessarily costly. Therefore, Commonwealth Bank considers that reciprocity should be an element of the CDR regime from its commencement.

The principles underlying an obligation of reciprocity should mirror that of the broader CDR regime – namely, that any requirement to share data would be at the request of the consumer. Any limitations on this element of the CDR regime should only be imposed in extraordinary circumstances, such as at the start of the lifecycle for a small fintech (see section 3.2 below).

As was recommended by the Final Report of the Review into Open Banking,[2] reciprocity obligations should be implemented as an extension of the accreditation process. That is, once a company applies to become an accredited data recipient, the Data Recipient Accreditor would conduct a review to consider whether the company collects any datasets that may be considered 'equivalent' would be subject to a reciprocal data obligation.

Where companies are operating primarily in the banking sector, the datasets naturally covered by a declaration of equivalence would mirror what has been included in the designation instrument.

3.1 Equivalence for non-banking participants

The Final Report of the Review into Open Banking recommended that as part of the accreditation process for *'data recipients that do not primarily operate in the banking sector, such as data recipients from the technology sector, the competition regulator should determine what constitutes equivalent data for the purposes of participating in Open Banking*'.

However, the task of defining 'equivalent' datasets should not be limited to what has already been outlined in the existing designation for a particular sector. This may lead to poor competitive outcomes and create an asymmetrical ability of accredited data recipients to generate new insights and services, as compared to the original data holder. This would lessen the benefits to the consumer as a result.

[2] Recommendation 3.9

Commonwealth Bank is of the view that the ACCC should therefore make rules that apply as part of the accreditation process to ensure that any self-nominating entity, wishing to become a data recipient, should agree to make available their core customer data to be shared at the consumer's request.

The ACCC should consider all core customer data that the data recipient would receive (within the scope of the designation instrument) and, additionally, any other data that it collects in order to deliver a service to the end user. This additional category of data should be included, so long as it broadly aligns with the enacted position on raw or derived data listed in the designation instrument, in the declaration of equivalence. The data recipient would also then become a data holder for the purposes of the regime, and would have to make available the equivalent datasets for the consumer to share in the CDR framework.

In other words, the Data Recipient Accreditor should be required to apply a test to the entity applying for accreditation such that if existing entities captured by a designation instrument were to compete with the newly accredited entity, what information would allow them to provide a competitive service to its consumers? This test would then 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.

3.2 Thresholds

There may be cases where the reciprocity rules should be weighed against other policy objectives, such as encouraging competition. The Government has already announced measures to encourage the development of smaller fintechs, such as tax incentives, grants and access to the ASIC regulatory sandbox. Commonwealth Bank supports creating thresholds, under which accredited data recipients would be given relief from reciprocity obligations. Such thresholds should be aligned with accepted definitions of 'small business', such as those in the Code of Banking Practice.

Recommendation 7:

The ACCC should introduce an equivalence test as part of the accreditation process, to be applied to any entity applying to become an accredited data recipient under the CDR framework. The ACCC should not be bound by the data listed in the existing designation instrument with respect to reciprocity but should instead enquire about the types of core data necessary to the provision of a service. Any accredited data recipient (subject to the limited exception in Recommendation 8) should make their core customer data available to be shared under the Rules at the consumer's request.

Recommendation 8:

A general exemption to reciprocity requirements should be granted to small businesses (including all related bodies corporate). Such thresholds should be aligned with accepted definitions of 'small business', such as those in the Code of Banking Practice.

4 Accreditation

4.1 Accreditation tiers

Commonwealth Bank is supportive of the development of a tiered accreditation where there has been a thorough risk assessment to share less-sensitive data. This should not apply to an intermediary model (as envisaged in section 12.1.3 of the Rules) until industry has decided on more fundamental issues about how an intermediary model should operate (such as the types of data that could be shared and on which terms, under the model).

Access to customer data, including transaction history, should be considered the most sensitive category of data to share under the CDR framework and should naturally require the highest tier of accreditation for data recipients.

4.2 Ongoing information security obligations

Commonwealth Bank welcomes robust measures to ensure ongoing compliance with accreditation standards and industry best practice cyber security standards (recognising that these standards will continue to evolve over time).

Three tangible steps should be taken to ensure ongoing compliance with information security standards.

Firstly, a 'reasonable steps' provision should be included to allow data holders to withhold data from accredited data recipients if they believe those third parties are not taking 'reasonable steps' under Section 20Q of the Privacy Act to protect customer security. This mechanism would operate in a similar manner as to the operation of the draft mandatory Comprehensive Credit Reporting legislation. Under this model, if the regulator does find that the third party had, in fact, taken 'reasonable steps' then the data holder would be penalised for non-compliance with the CDR regime.

Secondly, given the dynamic nature of cybercrime, annual attestation may be a helpful approach in encouraging participants to maintain adequate cyber defences. This approach would work with a principle-based approach to regulation, such as that taken in APRA's proposed Prudential Standards CPS 234.

Draft prudential standard CPS 234 (Information Security) is technology agnostic and principles-based, focusing on ensuring entities understand their information assets and the threats and vulnerabilities to which they are exposed, and have controls in place that are commensurate to those threats and responsibilities. Given the dynamic nature of cybersecurity threats, Commonwealth Bank favours an attestation procedure, whereby participants annually attest to their compliance with an agreed standard

And finally, the ACCC should look towards existing mechanisms for ongoing threat intelligence monitoring. The Australian Cyber Security Centre already plays an important role for facilitating the

sharing of threat intelligence between governments and private sector organisations, and would be well placed to have a formal role sharing data under the CDR.

Recommendation 9:

The Rules should include a 'reasonable steps' provision to allow the withholding of data by a data holder in the event that an accredited data recipient to whom the data holder would transfer data is found to have not taken reasonable steps to protect consumer data.

Additionally, an annual attestation for accredited data recipients should be built into the accreditation process to ensure compliance with industry best practice cyber security standards.

4.3 Revocation of accreditation

The ACCC envisages that, under the Rules, accredited data recipients will be required to report any material change in circumstances related to the grounds on which their accreditation may be suspended, varied or revoked.

In addition to the reportable matters outlined by the ACCC in the Rules, Commonwealth Bank supports exemptions from disclosure of CDR data by data holders in the Rules (in addition the exemption outlined in Recommendation 9):

a. if the data recipient no longer meets the accreditation criteria (including not maintaining appropriate security standards);
b. if a data holder reasonably suspects the accredited data recipient has suffered an unauthorised disclosure of CDR data; and
c. 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.

Commonwealth Bank recommends that the ACCC provide the above exemptions in the Rules, to ensure that data holders will not be liable for breach of its obligations under the CDR regime by suspending an accredited data recipient's access to CDR data in those circumstances.

4.4 Accreditation Requirements

Commonwealth Bank supports the use of the baseline criteria used in the EU Payment Services Directive No. 2 (PSD2) in the Rules.

The Rules sets out that applicants will also be required to be a 'fit and proper person', prove they have the appropriate and proportional infrastructure, demonstrate their internal dispute resolution processes meet the relevant requirements and hold appropriate insurance.

Commonwealth Bank strongly supports the requirement that accredited data recipients have insurance as a prerequisite of accreditation. This will help ensure that accredited data recipients have adequate

resources to promptly notify customers in the event of a data breach, thereby enabling customers to take steps to limit resulting damage and ensuring consumers can be compensated where appropriate.

Insurance providers now appear to be working with technology companies to leverage their knowledge in customer use cases and software and hardware vulnerabilities, and the cyber risk insurance market is rapidly maturing globally (influenced by the development of data regime, such as PSD2 in Europe).

The current draft Rules do not make provision for recognition of accreditation obtained by related bodies corporate of CDR participants. The requirement for all related bodies corporate of an accredited data recipient to become accredited may create unnecessary compliance costs and burdens if the corporations proposing to be accredited data recipients share the same security controls as the CDR participant.

Commonwealth Bank suggests that introducing recognition for related bodies corporate in these circumstances would practically benefit the CDR regime and support the underlying purpose of consumer choice and freedom. Commonwealth Bank also suggests the ACCC clarify whether the proposed streamlined accreditation process for ADIs will also apply to ADI subsidiaries.

Additionally, there are several ways that fraud could occur such as a data sharing relationship being established by fraudsters imitating a legitimate accredited data recipient or an employee of an accredited data recipient requesting access to a data holders developer environment who is not authorised to access this data.

The following is proposed to ensure that only authorised users will obtain access to API keys via a data holder's developer environment:

a. As part of the accreditation process the accredited data recipient nominates the employees who will be eligible to access the developer environment.
b. The ACCC is provided basic contact information including full name, title, business email and business phone number for each such eligible employee.
c. There should also be a requirement to provide information which enables a data holder to verify the identity of these employees, such as a HR contact phone number at the accredited data recipient organisation.
d. If any new employee of the accredited data recipient requires access to the developer environment, their details should be updated with the ACCC by the accredited data recipient. This process should:
    (i) require a thorough identification process completed with ACCC to ensure the applicant does in fact work for the accredited data recipient organisation; and
    (ii) have the ability to control which employees within the organisation had access to the API keys that are provided to access CDR data, however this may not be possible if keys are shared within the organisation.
e. The data holder would then be able to:
    (i) verify employee information provided against employee information held by the ACCC. This step could include sending a verification email to the listed email address (which would belong to the accredited data recipient organisation's domain) to ensure that the applicant does indeed have access to that address; and

(ii) contact the accredited data recipients nominated contact (such as HR) to confirm that this person should in fact be requesting access.

Another way that fraud could occur is if a company intending to commit fraud manages to achieve accreditation as an accredited data recipient. With the use of social engineering they may be able to convince consumers that they are offering a legitimate service and convince the customer to provide the consent for data sharing via the data holder. In order to mitigate this risk, as part of the accreditation process, the Data Recipient Accreditor should:

a. complete or obtain evidence of due diligence including criminal background check; and
b. review ASIC databases (e.g. companies you should not deal with) for negative records of companies / company directors.

Another scenario where an individual could attempt to access customer data fraudulently involves them completing an Identity Take-Over of an approved employee at an accredited data recipient and then accessing a data holders developer environment. To prevent this scenario occurring, access to an API key should only allow access to shared data within the infrastructure of the accredited data recipient.

As an example – if an individual was to conduct an Identity Take-Over of an authorised employee of company XYZ and gained access to the API key provided by Commonwealth Bank, this key should not allow the individual to access any customer data that has been shared between Commonwealth Bank and company XYZ as the individual does not have access to company XYZ's internal systems.

5 Consent requirements

5.1 Complex personal accounts

Commonwealth Bank acknowledges and supports the proposal by the ACCC to make rules which will require each party to an account to be notified of any data transfer arrangements initiated on their account. However, Commonwealth Bank recommends seeking consent from all account holders, even for 1-to-sign accounts. There are a large number of cases where sharing data among all account holders might infringe on privacy laws and capturing of consent for these account types is appropriate.

Limitations and timeline

The difficulty in delivering consent structures has less to do with the product design than it has to do with the complexity of authorisation hierarchies. Where there are complex authorisation hierarchies, it should not be assumed that any party who could theoretically access data today should be able to do so to exercise rights or fulfil obligations under the CDR regime. This is because access to data under the CDR regime assumes the ability to on-share with accredited data recipients, which increases the potential costs and liability of that data being misused.

Recommendation 10:

Commonwealth Bank has identified a number of complex authorisation structures which should be carved out of the first version of the Rules. Commonwealth Bank considers that these types of authorisation structures should not be brought within scope of the CDR regime at the commencement of the regime. These authorisation structures include:

a. complex personal accounts (e.g. deceased estates); and
b. individuals acting on behalf of consumers, such as authorised signatories

5.2 Complex business accounts

Commonwealth Bank recommends that the Rules not specify how data holders manage authorisations for business customer entities. Currently, data holders manage complex delegation structures as per their customers' requirements. These vary across the industry, and require data holders to make risk-based decisions on who may authorise payments and service activities. The same principle of customer choice should apply to the CDR framework.

Physical documents may be required to authorise data sharing on behalf of some business customers, e.g. board approvals/trust deeds used to bind an entity. It is common for corporate customers to provide paper-based authority documents, which are manually inspected before each transaction and are not digitally intelligible.

There also may be complications related to the legal entities of large business customers, some of which may be outside Australia. For example, consent may be given regarding a basic transaction

account but this may be tied into another product for which the individual cannot give consent or may inadvertently disclose material non-public information or have international regulatory implications.

Additionally, many transactions may involve multiple parties, for which gaining consent from one party may not be an appropriate means of obtaining consent (for example. securitisation for institutional clients). Such complex transactions should be carved out of the CDR regime.

Commonwealth Bank recommends that, in respect of business entities and non-human legal persons, only simple single account holders should be in-scope for the initial phase of the CDR regime, as consent can be sought from a single individual. A phased approach such as this could be adopted to deliver value for small business customers earlier, while the complexities of larger entities are worked through.

Recommendation 11:

Commonwealth Bank recommends that the ACCC adopt a phased approach to implementing business accounts focused on simple businesses first.

Complex business entities (e.g. large companies and associations) and multi-entity corporate structures (e.g. partnerships, trusts, JVs, SMSFs) should not be included in the CDR regime at its commencement. The ACCC should only include rules for the inclusion of these entities, after thorough consideration of issues including: appropriate controls for the sharing of sensitive commercial data; and managing complex consent structures; and the protection of intellectual property.

5.3 Children and minors

Commonwealth Bank considers that accredited data recipients should not be permitted to obtain consent from a CDR consumer where they should reasonably expect that a person is unable to provide informed consent. Additional consideration should be given to the treatment of children under the age of 18 and whether they sufficiently understand the risks of sharing data on their account.

The ability for children under the age of 18 to provide truly informed consent is diminished and many forms of contracts cannot legally be enforced against children. Generally, a contract made by a child under the age of 18 is voidable, unless it is a contract for necessities or a beneficial contract of employment. Furthermore, in NSW a child under the age of 18 is not bound by a contract except as provided for by legislation and even beneficial acts presumed binding will not be binding where the minor lacks the understanding 'necessary for his or her participation' in the act.[3] More generally, the OAIC Guidelines on the Australian Privacy Principles determine that a child under the age of 18 is only deemed to have capacity when they have sufficient understanding and maturity to understand what is being proposed.[4]

[3] *Minors (Property and Contracts) Act 1970* (NSW) ss 17-19.
[4] Office of the Australian Information Commissioner, 'Australian Privacy Principles guidelines – Privacy Act 1988', B.51, https://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/app-guidelines/APP-guidelines-combined-set-v1.pdf

Commonwealth Bank offers children full access to digital assets from the age 14, however, unless proactively removed from the account, parents continue to have access until age 18. Enabling minors to be included as CDR consumers would also facilitate the sharing of data beyond the primary account held by the child, and such transactions have the potential for harm, including infringements of privacy.

Given that consent from the CDR consumer is the touchstone of the valid exercise by an accredited data recipient of access to the data, and it is not practicable or reasonable for CDR participants to assess the capacity of children under the age of 18 to consent on a case-by-case basis, Commonwealth Bank recommends that, similar to the approach taken by the OAIC:

a. a CDR participant may presume that an individual over the age of 15 has the capacity to consent, unless there is clear evidence to suggest otherwise; and
b. children under the age of 15 should not be presumed to have the capacity to consent, and should therefore be excluded from the scope of the CDR regime. 5

Commonwealth Bank's recommendation is also consistent with the threshold ages of digital consent (between 13 and 16) being imposed by EU Member States to bring their national privacy legislation in line with article 8 of the EU General Data Protection Regulation.[6]

Recommendation 12:

Children and minors should not be included in the definition of CDR consumer.

5.4 Prohibitions on on-selling and direct marketing

Commonwealth Bank strongly opposes on-selling of data and would not support the CDR regime to be extended to allow this under any circumstances. As the regime develops, there may be some use cases where direct marketing is acceptable – for instance, a Personal Financial Management tool making recommendations for specific products. But this would need to be considered over time, after consideration of privacy impacts for customers and within well-defined legal principles and consumer protections.

[5] Office of the Australian Information Commissioner, 'Australian Privacy Principles guidelines – Privacy Act 1988', B.52, https://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/app-guidelines/APP-guidelines-combined-set-v1.pdf

[6] Centre for Information Policy Leadership, 'GDPR Implementation In Respect of Children's Data and Consent', 6 March 2018, 3, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_gdpr_implementation_in_respect_of_childrens_data_and_consent.pdf

6 Authorisation and authentication process

6.1 General obligations

In the Rules (section 8.3.1), it is not clear if each specific consent to a use or disclosure needs to be independent of any other use or disclosure, as well as independent of any other condition such as a product purchase.

Recommendation 13:

Consent for uses of CDR data should be unbundled so that each specific consent to a use or disclosure needs to be independent of:

a. any other use or disclosure; and
b. any other condition, such as a product purchase.

6.1.1 Authorisation in accordance with technical standards

The draft Rules includes a requirement that '*data holders must not add requirements to authorisation processes*'. Where consent to share requires re-verification of the customer's identity or action by the customer to improve the quality or accuracy of records, such as updating the officeholders linked to a business customer entity, these should not be regarded as unauthorised additional processes as they are required to ensure the data holder has appropriate records and verification on file to enable disclosure of CDR data. Re-verification is also required to meet a data holder's other regulatory obligations.

The draft Rules expresses the ACCC's intention to prohibit data holders from requesting additional information beyond what is described in the Rules or standards as necessary to authenticate the consumer and the consent they have agreed with the accredited data recipient. Commonwealth Bank is concerned that this prohibition does not allow for sufficient flexibility in circumstances where data holders may have grounds to suspect that the person requesting the CDR data is not the consumer and would require additional information for verification of the consumer's identity, or where more advanced authentication methods have been developed and have not yet been reflected in the Rules or standards.

Recommendation 14:

Commonwealth Bank recommends that the ACCC does not make rules prohibiting data holders from requesting additional information beyond what is described in the rules or standards.

6.1.2 Duration of authorisation

Commonwealth Bank supports the same framework and processes be applied each time consent is provided – that is, for collecting initial, and repeat, consents. The current timeframe of 90 days is an appropriate protection for consumers to provide ongoing consent. Commonwealth Bank recognises

that in the future there may be use-cases that may require further consideration of the duration of consent for those uses, however, at the outset of the regime customer security should be given primacy.

Additionally, the full consent process should be repeated each time there is a change of data uses by an accredited data recipient. For example, if a consumer submitted a loan application using data that was provided for the purposes of a Personal Financial Management tool only, that secondary use should be captured by an additional consent provided by the consumer.

7 Providing consumer data to consumers

The right for consumers to request direct access to CDR data should be included in the Rules but Commonwealth Bank's view is that the method of providing such access should not be prescribed. Data holders should have the flexibility to determine the methods offered for CDR consumers to access their own CDR data.

In many cases, data holders may offer existing services that meet this requirement and this will vary by the sophistication of the customer and the nature of the banking relationship. In terms of providing the capability to directly ingest data into their systems via an open API, this is a functionality that would only apply to the largest business customers and those customers are generally already served by sophisticated insights and data analytics services. As such, it is not necessary to provide this additional build requirement and, at the very least, it should not be included for the first two years of the CDR regime.

Recommendation 15:

Data holders should not be required to allow consumers to access CDR data via an open API as this would lower security standards, may lead to negative customer outcomes such as additional third parties requesting access to the APIs, and would involve a significant IT build requirement.

8 Use of Data

The Rules contemplates permitting CDR data to be shared outside of the CDR framework in certain prescribed circumstances. Commonwealth Bank believes this should be considered only in exceptional circumstances in which there is a strong public benefit for being able to do so.

The ACCC envisaged three use cases for where such an outcome may be permissible:

a. sharing to non-accredited persons, such as cloud accounting software providers sharing consumer data with accountants;
b. the provision of CDR data to intermediaries;
c. the provision of CDR data to non-accredited persons, such as contractors and outsourced service providers.

Each use case is addressed in the sections below. However, it is also worth outlining general principles for how Commonwealth Bank considers CDR data being sent outside of the CDR framework should be dealt with.

Firstly, Commonwealth Bank considers there should be a general principle that the on-sharing of CDR data from an accredited data recipient should not result in an increased security or privacy risk to the consumer; this should also be true of data being shared outside of the CDR regime.

Secondly, any solution needs to be designed tightly to prevent such an ability to share being used as loopholes for purposes other than those envisaged by the ACCC.

Thirdly, so long as an accredited data recipient is sharing data outside of the regime, it does not mean that the CDR consumer protections no longer apply to that CDR data simply because the CDR data has been on-shared or the means to sharing has changed. Accredited data recipients should have a strong role to play in monitoring and governing the use of CDR data they receive on an ongoing basis, and they should use contractual and technical arrangements (such as user access management) to enforce important consumer protections under the CDR regime and other safeguards. In such cases, liability should not move with the data; the liability and responsibility to ensure that data is used within the constraints and spirit of the CDR regime should sit with the last accredited data holder.

8.1 Disclosure of consumer data to other parties for use by those parties

Commonwealth Bank believes that if accredited data recipients are able to transfer data to non-accredited persons, even if directed by a consumer, this would weaken the integrity and trust in the CDR regime. Such a system would also be particularly vulnerable to being used as a loophole for companies to share large quantities of consumer data outside of the CDR framework in a way inconsistent with consumer consent and the general principles of the CDR regime.

8.1.1 Conditions

Commonwealth Bank considers that if CDR data is to be shared with non-accredited persons, there should be several conditions to the disclosure that could bolster the integrity of this model:

a. Under no circumstances should an accredited data recipient profit from sharing CDR data outside of the CDR framework.
b. Raw data should stay with the CDR participant that has the higher accredited standard. Insights or derived data could be shared with a lower tiered accredited participant for the use of such insights, (as distinct from where a non-accredited person is acting on behalf of the consumer, for example in agency / professional relationship – see below) without the raw data being shifted from the higher security environment.
c. Express consent should be captured by the accredited data recipient, such as an accounting software provider, for CDR data to be shared with a non-accredited person and the uses that apply to the CDR data should be agreed to and similarly captured.
d. The consumer should be able to revoke a non-accredited person's access to their CDR data and require the non-accredited party to delete any of that CDR consumer's CDR data that they hold. These rights should be enforced through ordinary commercial agreements that the accredited data recipient must enter into with the non-accredited person.
e. The accredited data recipient should have a positive obligation to inform the CDR consumer that the data is going outside of the CDR framework and is not subject to the CDR protections.

8.1.2 Requirements

Commonwealth Bank proposes that the CDR regime should impose requirements for disclosures to non-accredited persons. This could occur through:

a. 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. requiring accredited data recipients to take reasonable steps to ensure that non-accredited persons do not breach the CDR regime. Under this model:
    (i) the accredited data recipient would be required to take reasonable steps, including in any terms and conditions that apply to a data transfer to a non-accredited persons, 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;
    (ii) the CDR consumer should be entitled to complain to OAIC for misuse of data by non-accredited persons; and
    (iii) the accredited data recipient is liable for the acts or omissions of any non-accredited person to whom that accredited data recipient transferred CDR data and that contravened the CDR regime in relation to that CDR data, 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 persons to incentivise accredited data recipients to flow down their obligations under the CDR regime to non-accredited persons through contractual arrangements.

The pre-requisites of an alternative accreditation tier would need to be set at appropriate levels to the types of entities from whom it was proposed were proposed to obtain CDR data.

Some benefits of this alternative approach might include:

a. Education: Ability to educate additional non-accredited persons (e.g. accountants) about their responsibilities to store and use data appropriately.
b. Efficiency: Over time, it could be easier for an accountant to go through one accreditation process, as opposed to signing contracts on a case-by-case basis with multiple providers of CDR data.
c. Integrity: Stops leakage of CDR data and ensures that CDR data is only used in accordance with the CDR consumer's consent.

Commonwealth Bank does not support either approach being taken in the initial stages of the CDR regime. Industry should work on solutions to protect consumers and the integrity of the CDR framework before any solutions are adopted.

8.2 Provision of CDR data to intermediaries

The provision of CDR data to accredited intermediaries acting on behalf of accredited data recipients will create additional complexity and responsibility for data holders to verify that the accredited intermediary is in fact acting on behalf of the accredited data recipient during the authentication process.

The involvement of intermediaries will also create additional complexity regarding the consequences of suspension or revocation of accreditation for intermediaries and accredited data recipients. If an intermediary's accreditation is suspended or revoked, in some circumstances, this may require the accredited data recipient that is using the intermediary to have its accreditation suspended or revoked, and vice versa. For example, where an intermediary has knowingly been providing CDR data to an accredited data recipient that has breached the Privacy Safeguards or has committed an offence of dishonesty, then both the intermediary and the accredited data recipient should have their accreditation suspended or revoked.

Recommendation 16:

Given the complexity of issues surrounding the inclusion of intermediaries into the CDR regime, intermediaries should not be included in the regime for the first 24 months of operation. Industry should use this time to work to solve problems around data collection, use and on-sharing, consent models, accreditation tiers and information security standards.

8.3 Provision of CDR data to outsourced service providers

Commonwealth Bank recommends that the ACCC make rules which allow for the disclosure of CDR data to a service provider of the accredited data recipient for the provision of services to such accredited data recipients which are within the scope of the purpose for which the CDR data was provided by the accredited recipient to the service provider.

This should only be permitted where the on-sharing of data is required for the purpose of providing the service to which the CDR consumer has consented (for instance, if the service provider is providing data storage and information security services in support of the services being provided to the CDR consumer by the accredited data recipient).

Commonwealth Bank supports the ACCC's intention to make rules that require an accredited data recipient to ensure it has appropriate plans and processes in place for managing risk associated with any outsourcing arrangements involving the disclosure of CDR data. For example, the accreditation process could require the accredited data recipient to undertake due diligence of the proposed service provider's information security systems and establish procedures for the data recipient's continual monitoring performance of the service provider under the outsourcing agreement.

Recommendation 17:

The ACCC should make rules that include:

a. an accreditation framework which sets the technical and organisational measures which an accredited data recipient must implement to address security (including with respect to its employees and the security of its suppliers and their subcontractors); and
b. standards no lower than ASIC's RG 104 and APRA's CPS231, and similar guidances, and apply those 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.

9 Operation of the privacy safeguards

Commonwealth Bank supports strengthening consumer privacy protections to ensure consumer information is handled appropriately.

Particularly, the requirements for collection, use and disclosure of CDR data are important safeguards for individuals and businesses.

However, Commonwealth Bank's view is that to the extent possible, the Privacy Act and the Privacy Safeguards should be aligned and consistent. Commonwealth Bank notes that, since the release of the Rules, new Privacy Safeguards have been proposed in a second exposure draft of the Bill. However, Commonwealth Bank considers that the Privacy Safeguards still add complexity and uncertainty for participants and consumers.

Commonwealth Bank suggests that, to the extent possible, the scope of the Privacy Safeguards be further clarified to reduce complexity and avoid significant extensions of privacy law. Commonwealth Bank notes that the Bill provides the ACCC with the power to make rules on when CDR participants will be compliant with the Privacy Safeguards and suggests that the rules made by the ACCC be consistent with this approach.

9.1 Safeguard 1: Open and Transparent management of data

The ACCC proposes making rules regarding the form and information to be contained in a CDR participant's CDR policy including a list of outsourced service providers, the nature of their services, and the data that has been disclosed to them. It is unclear what policy objective is being achieved by requiring disclosure of this level of detail.

While it may be relevant for a CDR consumer to understand if a CDR participant uses third parties to support the systems which hold and process CDR data, Commonwealth Bank considers it unnecessary and unwieldy to provide such a level of detail and obtain express consent for such a disclosure. Further, given that it would likely be difficult, if not impossible, to process CDR data without such systems, we query how a CDR participant would manage a circumstance where a CDR consumer failed to provide consent for the disclosure.

9.2 Safeguard 2: Anonymity and Pseudonymity

The revised privacy safeguards require accredited data recipients to transact pseudonymously or anonymously with them, unless the Rules provide otherwise. The safeguard does not follow the language of the corresponding APP 2 which allows an exception to this requirement where required by law or if impracticable to do so. If the final form of the safeguard is not modified to align itself with APP 2, then Commonwealth Bank recommends the ACCC extends its proposed rule to cover both anonymity as well as the currently proposed pseudonymity, possibly by allowing this approach on the same grounds as APP 2, given it is not known what services the accredited data recipient will be providing the CDR consumer.

9.3 Safeguard 4: Unsolicited data

Commonwealth Bank recommends that the ACCC make rules which provides an exemption from complying with Privacy Safeguard 4 for the sharing of CDR data between a data holder and an accredited data recipient that is a related body corporate of the data holder (i.e. where the accredited data recipient is required to use the CDR data for the purposes requested by the CDR consumer but is not the entity that solicited the data). Commonwealth Bank believes that this exemption is necessary to ensure that corporate groups can conduct their business and provide products and services to CDR consumers without unnecessary restriction of data sharing between related bodies corporate. This exemption can be equivalent to the right to transfer personal information between related bodies corporate under section 13 of the Privacy Act.

9.4 Safeguard 5: Notifying the collection of CDR data

Commonwealth Bank supports the proposed list of information which the ACCC proposes to require that accredited data recipients disclose to CDR consumers as part of the consent process. However, Commonwealth Bank believes that, in order to ensure consistency between the Privacy Act and the Privacy Safeguards, the information required in APP 5 for notifying individuals should also be included in the Rules for Privacy Safeguard 5. APP 5 requires that an accredited data recipient also include its contact details when notifying individuals of the collection of their personal information, whereas in the draft Rules, the accredited data recipient need only provide their name.

Commonwealth Bank fully supports the ACCC's intention to make rules requiring data holders to inform CDR consumers that their relationship with the accredited data recipient does not involve the data holder and the sharing of data is at the consumer's risk. Commonwealth Bank suggests that in order to ensure consistency in notifications between data holders and accredited data recipients, that accredited data recipients should also be required to notify CDR consumers that their relationship does not involve the data holder, and that the data holder's sharing of CDR data with the accredited data recipient is at the consumer's own risk.

9.5 Safeguard 6: Use or disclosure of CDR data

Commonwealth Bank is concerned that Privacy Safeguard 6 will require consent for all uses or disclosures, when it may be too stringent to expect seeking consumer consent in some circumstances. Commonwealth Bank recommends that exceptions to the consent requirement be set out in the Rules to address the types of disclosures by accredited data recipients 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). The exceptions to the consent requirement for use or disclosure to outsourced service providers should only apply where accredited data recipients have complied with the requirements in the Rules and the accreditation process regarding disclosure to outsourced service providers for managing risk (see section 8.3 above in this submission).

9.6 Safeguard 8: Cross-border disclosure of CDR data

The drafting of Privacy Safeguard 8 permits the ACCC to make conditions in the Rules for the transfer of CDR data overseas by accredited data recipients. The Rules states that the ACCC does not propose to make any additional requirements for the transfer of data overseas, due to the stringent rules on consent. The current approach under APP 8 in the Privacy Act is for the transferring entity to accept liability for any acts or practices of the overseas recipient which are in breach of the APPs as if the transferring entity had breached the APPs itself. Commonwealth Bank suggests adopting this approach for Privacy Safeguard 8 which then provides consumers and regulators with direct, locally enforceable rights in the event of a breach by an overseas party.

9.7 Safeguard 10: Notifying of the disclosure of CDR data

Commonwealth Bank notes that Privacy Safeguard 10 requires data holders to notify CDR consumers for CDR data of a valid request from a CDR consumer for that CDR data. Commonwealth Bank recommends that the Rules clarify how this Privacy Safeguard can be complied with for persistent authorisations, where it will not be practical for data holders to notify those CDR consumers multiple times for a continuous data feed for the period of authorisation. In such circumstances, Commonwealth Bank recommends that the Rules allow for data holders to satisfy their obligation to notify CDR consumers once when data sharing feed is initiated for persistent authorisations for the period that the authorisation is valid and for the particular purpose.

9.8 Safeguard 12: Security (de-identification and deletion)

Requirements to delete data should align with existing obligations and accommodate Australian and international regulatory requirements to simplify the complexity for data holders acting in the capacity of accredited data recipient and to assist customers in understanding their rights.

10. Dispute resolution

Commonwealth Bank is supportive of the ACCC's intention to require that all CDR participants have internal dispute resolution procedures in place, as well as the recognition of the Australian Financial Complaints Authority (AFCA) as an external dispute resolution scheme for the banking sector.

Larger businesses have sophisticated commercial and legal teams that are not at a disadvantage when dealing with financial institutions, and therefore it is appropriate that such entities would have recourse to courts, rather than an external dispute resolution scheme. On this basis, Commonwealth Bank does not believe that mandating alternative dispute resolution in the Rules is necessary, given the existing statutory requirements for courts to refer disputes to alternative dispute resolution procedures.

11. Liability

Commonwealth Bank notes the ACCC's intention to make rules requiring an accredited data recipient that is a foreign entity to appoint a local agent that will be responsible for any obligations of the foreign entity under the CDR regime and may be liable for any breaches or penalties. This requirement differs from the requirement under the Corporations Act for registered foreign entities to appoint a local agent, given that the Corporations Act requires that foreign entities 'carry on business' in Australia in order to register as a foreign company, whereas under the Bill, foreign entities with little or no presence in Australia may be subject to the CDR regime.

In the proposed circumstances, a local agent would be liable for any breaches or penalties. Under agency law, the appointed agent of the foreign entity would be entitled to an indemnity from the foreign entity against all liabilities, but it is more appropriate that it is enforced directly against the accredited data recipient. Furthermore, the appointed agent would only be liable for breaches or penalties of the foreign entity and not the outsourced service provider.

With respect to liability to disclosures to non-accredited persons refer to section 8.

Recommendation 18:

Foreign entities seeking accreditation under the CDR regime should be required to register under the *Corporations Act 2001* and to be required to provide security for performance such as a bank guarantee or performance bond.

Further, an aggrieved party should have recourse for any claim it has against the accredited data recipient through either the local agent and the principal.