Commonwealth Bank
Commonwealth Bank of Australia
ABN 48 123 123 124

Inquiry into Future Directions for the Consumer Data Right

Introduction

Commonwealth Bank supports the Consumer Data Right

Commonwealth Bank appreciates the opportunity to make this submission in response to the Treasury's Inquiry into Future Directions for the Consumer Data Right (CDR) Issues Paper published March 2020.

Commonwealth Bank welcomes the Treasury's Inquiry to consider the future purpose, use and vision for the CDR in Australia. Commonwealth Bank believes that giving Australian consumers and businesses greater control over access to their data in a safe and secure manner has the potential to enhance the wellbeing of consumers and to foster a strong and innovative digital economy.

The Government's intention, as stated in the Issues Paper, is to enhance and leverage the CDR "*to boost innovation and competition, and support the development of a safe and efficient digital economy, benefiting Australians and Australia"*[1]. Commonwealth Bank is fully aligned with these objectives. Furthermore, Commonwealth Bank believes that an enhanced CDR regime offers an opportunity to better protect Australian consumers online through improved cyber security controls for electronic data exchange across Australia. This will ensure that the CDR achieves sustainable benefits for competition, innovation and productivity.

To ensure that the efforts expended on Open Banking can be leveraged, Commonwealth Bank believes that the following common principles should be adhered to:

Firstly, CDR reforms should result in Australia and Australians being better off. This means ensuring solutions provide consumers the productivity benefits associated with greater access to data without increasing their exposure to misuse or mishandling of data. To achieve this, reforms must be designed with a view to raise consumer awareness and place consumers in control over access to their data. Further, where industry frameworks currently being developed are fit for purpose, additional regulatory intervention is not necessary to support better consumer outcomes.

Once the CDR regime is active and able to facilitate safe data sharing in the economy, Commonwealth Bank strongly recommends that unsafe data sharing practices, such as screen scraping, be prohibited, as these practices co-existing will cause consumer confusion and may increase the level of unsafe credential sharing. Ensuring customer data can only be accessed through the CDR in a manner that puts consumers in control and provides them with both privacy and financial protection will be critical to ensuring both uptake of the regime and the

[1] Treasury, *Inquiry into the Future Direction of the Consumer Data Right – Issues Paper,* p 1

reduction of poor customer outcomes that result from non-permissioned use or inadequate operational processes.

Secondly, there should be clear incentives for existing market players as well as new entrants to participate. Commonwealth Bank is firmly of the view that the CDR's data sharing framework should be based on principles of safety, security and reciprocity. Participants seeking access to consumer data should be prepared to (i) meet high levels of operational integrity and (ii) be prepared to share data when requested by consumers.

Thirdly, frameworks need to be interoperable across industries. Standardising data sharing standards and processes across industries is consistent with the core principles of data portability, and will reduce transaction costs for consumers in using their data across the economy (for instance in enabling energy providers to recommend a customer new ways of paying for their energy bills, or by helping banks provide insights to a customer on their energy usage).

The proposals contained in this submission will assist Government to deliver on its promise to implement a sustainable and comprehensive CDR framework for the Australian economy. Commonwealth Bank would like to recommend that Government consider the initiatives outlined below.

Section I - Future role and outcomes of the Consumer Data Right

Providing greater volumes of consumer data from across industries would provide greater incentives to consumers to participate in the CDR regime, resulting in greater business and consumer take-up.

Commonwealth Bank holds the firm view that the principle of reciprocity is key to creating a 'network effect' to quickly advance the successful implementation of the CDR and ensure the CDR fosters a dynamic and world-leading data sharing regime that brings the greatest benefit to Australia and Australian consumers. The concept of reciprocity should be broadened to ensure that those receiving data and benefitting from the regime are also subject to its obligations to share data, if directed to do so by consumers.

Reciprocity of data sharing will deliver the greatest benefit to Australia and Australian consumers and is a core principle of data portability. There would be significant benefits for consumers if they were able to choose to share their data from one company to another, however currently there is no incentive for companies in non-designated sectors to enable this consumer benefit. Further, reciprocity of data sharing is critical to ensure Australian businesses can remain competitive in the digital economy and to avoid an asymmetry between the obligations on data holders and ADRs. For example, the current lack of reciprocity for non-designated sectors adversely impacts the ability of Australian businesses to compete with international tech giants who could access CDR data sets but are not required to share their own data sets. This would allow these businesses to consolidate their position and practices as data companies by overlaying their existing data insights and analytics while the lack of reciprocity would limit the ability for data holders in Australia to compete on a level playing field.

Commonwealth Bank recommends that all participants who are prepared to ingest consumer data through the CDR regime should be required to reciprocate, irrespective of whether those entities are within a designated sector. The principle of reciprocity will ensure all participants are incentivised to deliver the right outcome for consumers.

To enable reciprocity, the future accreditation criteria should, at a minimum, identify and include an obligation for ADRs to share any consumer data they propose to combine with data obtained under the CDR to develop a product or service, where the consumer has consented to that data being shared. The rules should be amended to enable CDR consumers to request data that is to be combined with CDR data under the rules be disclosed to the consumer or an ADR under Part 3 and 4 of the CDR Rules. The CDR Rules should be amended further to require ADRs to maintain information on their websites about the data available to CDR consumers in their capacity as reciprocal data holders.

Critically, the CDR Rules should be amended to specify that any entity ingesting data through the CDR regime is subject to data reciprocity, regardless of whether they fall within a designated sector.

Section II - International Context

International developments and the experience of other jurisdictions in implementing their open data agenda provides valuable insights for the design of Australia's data sharing regime. Key learnings include the need for practical implementation timeframes, a combination of regulatory and market driven approaches, and a consumer awareness program to encourage uptake.

While payments reforms in other jurisdictions can be a useful guide for domestic regulatory reform, it is important to differentiate the Australian payments system in order to understand whether overseas legislation is applicable or relevant to the Australian context.

A. Practical timeframes

Experience has shown that many jurisdictions have underestimated the complexity and scale of Open Banking implementation, leading to slippages in timelines. For example, only four of the UK's largest account providers were ready by the date mandated to launch their Open Banking initiatives and have continued to miss deadlines for ongoing delivery of Open Banking functionality.

Collaboration and co-operation across industry and regulators will be necessary to agree on practical implementation timeframes, and to facilitate appropriate planning and sequencing of multiple technological changes. The Australian payments industry in particular is currently facing unprecedented demands that should be taken into consideration, including major projects such as the New Payments Platform and SWIFT ISO20022 migration and the need to maintain resilience in the face of increasing demands on technology platforms. Further, greater coordination and planning would allow rules to be developed, and then standards to be developed and finalised before technical build within industries commences, which in turn reduces potential rework.

B. Mandated vs market based

The level of regulation to introduce Open Banking varies across jurisdictions, ranging from prescriptive and mandated implementation to facilitating a more market driven response. In the international context, Australia has adopted a more directed process to introduce Open Banking when compared to Hong Kong and Singapore - where recommendations have focused on open API designs and technical specifications to facilitate adoption of Open Banking practices.

In jurisdictions that have taken a regulatory approach to introducing Open Banking, the development of common standards has required consensus across many stakeholders with different underlying platforms, data models and security approaches. Therefore, Commonwealth Bank considers that where possible regulatory and technical frameworks should allow for the flexibility of industry and market driven solutions. We support the learnings from the UK's post-implementation review, which recommended Open Banking *'should provide a commercial incentive for banks to grow the Open Banking ecosystem and improve the performance of their APIs'*.[2] Further, while regulation does have a role to play in market failures, it is Commonwealth Bank's view that regulatory approaches should be balanced to ensure they do not impede growth and efficiency in the economy.

C. Consumer awareness

Building consumer trust and confidence will be critical for participation in Open Banking. Low consumer awareness has been a barrier to uptake in other jurisdictions. For example, a year after Open Banking was introduced in the UK, only 5 per cent of the public understood the initiative. This lack of understanding and confidence has undermined the UK Government's efforts to introduce an effective data sharing regime. Commonwealth Bank would encourage the government and the regulator to support education for consumers on the use and proposed benefits of the regime to increase confidence in the system. Commonwealth Bank continues to take proactive steps to elevate customer understanding of safe data sharing practices, based on existing Government standards as well as lessons from industry best practice.

Section III - Switching

Open Banking will give consumers greater control of their data held by banks, enabling the delivery of new services, increasing transparency and delivering more choice and competition among financial products. For example, the Australian implementation of Open Banking has included increasing access to headline product data such as published interest rates and terms and conditions. There are productivity benefits arising from making this information available in a standardised, easily accessible form. New market entrants will be able to create business models leveraging this data, enabling consumers to compare product offerings with increased accuracy.

We recognise further work needs to be done to determine the best way to enable consumers to switch products and providers within the CDR regime and ensure appropriate controls are in place to minimise associated risks.

Importantly, any model for switching needs to ensure consumer protection remains the core principle of the CDR regime. We recommend that in instances where it has been found that switching has occurred improperly, consumers should be able to reverse the action without being disadvantaged. To enable safer switching for consumers under the CDR, appropriate controls will need to be introduced to manage the combination of read and write access required (See Section VI for our specific recommendations on elements and controls required for write access).

Further, many providers are also subject to legal and regulatory requirements, for example contract law, when entering agreements with customers, which provide important protections for consumers. Any expansion of the CDR to enable switching would need to consider how the CDR would ensure these requirements are met.

[2] ODI & Fingleton, *Open Banking, Preparing for lift off*, 2019, p 5

Section IV - Read Access

A. Promoting broader access through tiered accreditation

Commonwealth Bank supports a robust accreditation process and a tiered accreditation model that reflects the risk profiles associated with expanded read and write activities, without relaxing the existing obligations concerning security, privacy and consumer consent. We note the recent ACCC consultation on facilitating participation of third-party service providers in the Open Banking regime. Commonwealth Bank had the opportunity to contribute to the ABA's submission to the ACCC's consultation, and we support the principles it articulates for the development of rules in the CDR framework to enable broader read access by third-party service providers.

B. A consent taxonomy

Commonwealth Bank supports the introduction of a consent taxonomy. A consent taxonomy will enable greater consumer control over the data they choose to share, by supporting more granular and precise consents. This will be essential to facilitate write access and the combination of read and write access, as proposed by this Issues Paper.

Furthermore, a taxonomy would provide greater standardisation, uplift programmatic interpretation of consent and support the liability and accountability framework, in turn boosting customer confidence in the CDR regime. Commonwealth Bank recommends that the descriptive language as well as the specific implications of a consent be standardised at a regime level.

C. Safely managing consents

In Australia's Open Banking regime, the consent management design plays a key role in ensuring consumers are in control of their data sharing. In the Open Banking regime, consumers must provide informed consent and determine what data to share as well as the purpose(s) for which the data is shared with an accredited entity. Consumers can view and manage their consents through the consent dashboards, including withdrawing consent at any time.

This strong focus on consumer consent places consumers' firmly in control of access to their data and provides a secure platform for the sharing of data. This approach will take the industry forward by removing the use of unsecure practices, such as password sharing and screen-scraping which the Basel Committee on Banking Supervision has referred to as *"unsecure for the customer, since the third party maintains the credentials that provide full access to the customer's account"*[3].

The Basel Committee also acknowledges that:

"Banks, third parties and regulators recognise the security and customer protection risks associated with screen scraping…. Third parties use [this method] to collect and store customer credentials (i.e., username and password), which could be stolen or misused, including for payment fraud purposes."

[3] Basel Committee on Banking Supervision, Report on open banking and application programming interfaces, 2019, p 9

"Screen scraping …can undermine a bank's ability to identify fraudulent transactions, as banks cannot always distinguish between the customer, data aggregator, and an unauthorised third party that is logging in and extracting sensitive data."[4]

Commonwealth Bank supports Open Banking becoming the platform adopted by all parties to share consumer data, and in turn, replace unsafe and unprotected practices that encourage consumers to share online banking credentials while also communicating that this is a low risk activity.

Commonwealth Bank's primary concern with screen scraping is the security issues it creates. It remains our firm belief that sharing usernames and passwords is a fundamentally unsafe practice, both in the signals it sends about the importance of these credentials, as well as the storage of these credentials outside the bank's ecosystem.

Key risks associated with handing over usernames and passwords, include unauthorised transactions and identify theft. Among other things, it provides:

- full access to all personal and financial information available for the consumer, including any superannuation, insurance and CommSec trading accounts regardless of the reason for a party seeking access;
- the ability to transact on bank accounts where multi-factor authentication is not required; and
- the ability to open new accounts on the customer's profile and in their name.

Screen scraping has been identified as a serious security risk and the European Union (EU) and the United Kingdom are working towards banning the practice. The EU's Second Payments Services Directive (PSD2) was developed to control digital capture practices by requiring banks to create dedicated infrastructure for the sharing of consumer data with third party providers and requiring stronger consumer authentication, which would prevent screen scraping from occurring.

Recent statistics released by the Office of the Australian Information Commissioner (OAIC) in its Notifiable Data Breaches Report[5], for the period July to December 2019, outline that:

- 64 per cent of notified breaches were due to malicious or criminal attacks including cyber incidents of which many have exploited vulnerabilities involving a human factor (such as clicking on a phishing email or disclosing passwords);
- 37 per cent of data breaches notified involved an individual's financial details, such as bank account or credit card numbers; and
- Finance is the second highest reporting sector, notifying 14 per cent of all breaches.

These statistics highlight the ongoing and increasing threat to Australians' personal information and reinforce the importance of protecting consumer data, including their log-on credentials.

In recognition of data security best practice, Open Banking, by design, does not allow password sharing. Allowing screen scraping to continue alongside the Open Banking regime will result in 'dual schemes' being in operation, to the detriment of consumers as well as take up and participation in the broader CDR regime. Customers who share data outside the regime will not be aware that they do not have the same consumer and privacy protections. Learning from the

[4] Basel Committee on Banking Competition, Report on open banking and application programming interfaces, November 2019, p 8

[5] Office of the Australian Information Commissioner, Notifiable Data Breaches Report: July-December 2019, 28 February 2020

UK, Commonwealth Bank strongly recommends the introduction of a sunset clause to prohibit the use of unsafe methods of data sharing.

D. Accelerating the creation of a safe and efficient ecosystem

To accelerate the creation of a safe and efficient ecosystem, consumers must have confidence in the security of the ecosystem and its participants. To ensure that the ecosystem remains safe and consumer confidence is maintained, Commonwealth Bank is firmly of the view that accountability for the end-to-end security of the ecosystem resides with the regulator, and regular independent security reviews of the ecosystem will be required as standards change and new use cases are introduced.

Commonwealth Bank supports the creation of a centralised CDR cyber-security capability across the respective CDR governance entities, which would be accountable for intelligence gathering and coordinating responses to incidents and data breaches. At this time, when a data breach occurs, entities frequently need to analyse the data itself to identify the organisation that was compromised, and to take the appropriate cyber actions to protect consumers. In order to more efficiently identify malicious attacks and breaches, Commonwealth Bank recommends that data holders are given permission to create "simulated" identities (e.g. synthetic customer profiles), with each holder being allowed to have a different set of identities for each recipient. Based on a full extract of the data, each holder could identify which third-party was compromised. This will enable faster identification of malicious attacks and data breaches to enable the regulator and participants to quickly identify and respond to incidents.

Section V - Write Access

A. Write Access - general comments

The proposed expansion of the CDR to include write access has the potential to drive economic benefit for consumers and the Australian economy, including increased competition, data-informed innovations for products and services, and a secure and efficient way for Australian consumers to consent to a trusted third party acting on their behalf.

Given this, the introduction of write access to Open Banking will need to be carefully managed to minimise the privacy, fraud and financial risks to consumers, particularly those most vulnerable, participants and the Open Banking ecosystem. Strong controls must be developed to ensure the system cannot be utilised to fraudulently access consumers' information, financial facilities and savings.

The changes required to enable write access in existing CDR systems and infrastructure will impact the core systems of data holders while also exposing data holders to additional threats to critical IT assets, storage capacity and computing capability. Additional controls such as strong input validation and sanitisation would be required to mitigate the risks of a participant injecting abnormal volume or malicious content into data holders' systems.

Given the current technical standards of the CDR were developed for read access only, Commonwealth Bank understands new technical standards would be required to support write access, including detailed security specifications. Commonwealth Bank strongly recommends the prioritisation of designing strong security controls to protect consumers from exposure to material risk associated with the introduction of write access.

The complexity and material risks of introducing write access into Open Banking cannot be understated. Careful consideration of the security measures, controls, technical standards and consumer protections is required for write access to deliver the potential benefits outlined in this Issues Paper.

Commonwealth Bank recommends that write access not be considered for inclusion in the CDR until a post-implementation review is conducted after the full implementation of the current CDR (Open Banking) regime as previously committed by the Government. This will enable the consideration and design of any future CDR policy to benefit from data-driven findings of the review, and have regard to industry innovation which has occurred in the interim.

B. Write Access – Security

In serving customers at scale, we see how devastating the impacts of fraud, cyber and privacy issues can be for customers. Protecting our customers' data is a responsibility we do not take lightly and, each year, we invest significantly in continuously improving our cyber security controls. This is in addition to continuously improving the security of our online banking applications, and our dedicated fraud monitoring and investigation teams who work 24x7. Our 100% security guarantee protects customers from unauthorised transactions on personal and business accounts when they take the necessary steps to stay safe online.

Due to differences in the underlying nature and risks associated with write access, there are additional cybersecurity controls that must be addressed before any consideration is made to expand the CDR regime to incorporate write access. For example, within financial services, cyber-attacks and fraud are currently minimised, and customers protected through a comparison of analysis done on end-user devices (e.g. a customer's online banking browser sessions and mobile banking applications) for the presence of malware, overlaid with back-end transactional history held by the customer's bank. This allows banks to identify cyber-attacks and potential fraud.

It is not yet understood how this monitoring could be facilitated within the current or future CDR, given only the ADR would have access to the telemetry indicating a compromised device, whereas the Data Holder processing the transactions has the transaction history. The growing sophistication of cyber-attacks requires constant defensive innovation, and device telemetry has grown from a minor component to the major source for identifying and preventing cyber-crime. This example, and other cybersecurity controls must receive due consideration prior to any expansion of the current regime.

To ensure the successful introduction of write access, the following key components will be required:

- Ensuring consumers are dealing with trusted entities by introducing a higher tier of accreditation that requires specific standards and obligations of entities seeking to use write access, given the potential fraud risks for consumers.
- Controls including multi-factor authentication and confirmation notifications (e.g. warning messages), and the extension of existing refusal to disclose exemptions for data holders to include refusals to give effect to write access where the data holder considers this to be necessary to prevent physical or financial harm or abuse.
- Point-in-time multi factor authentication, aligned to industry best practice, for particular high risk instances/ changes to account data such as making new payments and adding new beneficiaries.

- To ensure consumers have appropriate recourse for loss or misuse of CDR data, onus must be placed on ADRs accredited for write access to investigate and, where appropriate, remediate and/or reimburse any loss to consumers arising from use of their services. Further, the existing liability protection should be extended to CDR entities that allow write access in accordance with the Competition and Consumer Act and the CDR Rules. ADRs should not be permitted to contract out of, or limit, liability to consumers for losses arising from their platform. In order for this to be effectively applied, ADRs should be subject to equivalent rules relating to dispute resolution as contained in Part 6 of the CDR Rules. ADRs and their service providers will therefore be free to contract to apportion any resulting liability between them as appropriate.
- This liability and accountability framework should be supplemented by technical standards that include standard patterns and chains of trust for non-repudiation of write access instances. For example, if a write access action was later disputed by the consumer, non-repudiation standards would provide evidence for the dispute resolution process to determine if the write access occurred due to a failure by an ADR to adhere to the CDR Rules. The current CDR standards require future enhancement to provide for non-repudiation. Consent should be captured more often under the framework for write access.
- The development of a robust, standardised approach for collecting consumer consent and API calls for write access. A robust consent solution will be required to enable a non-repudiation mechanism and enable ADRs to securely communicate consent details with data holders, improving the likelihood of identifying potential attacks and malicious activities. Further, the introduction of more granular and precise consents will be a prerequisite for write access. We support the development of technical standards that align with existing industry best practice for fraud and cyber monitoring, detection and action measures.
- Accountability for end-to-end security of the CDR ecosystem residing with the regulator, with regular independent security reviews of the ecosystem as standards change and new use cases are introduced.

C. Write Access – personally identifiable information and consumer information

Where there are any requests to change personally identifiable information there is a very strong risk of misuse for fraud. For example, there is a material risk of criminals targeting a consumer's mobile phone number to conduct fraud, as control of the mobile phone number can lead to control of an account. Further, ecosystem-wide security and fraud risks would be created, as the interconnected nature of the Open Banking ecosystem means that it in the event a single ADR had weak security processes this would be used to target a high number of consumers across a range of financial institutions. There are also additional security risks that arise in relation to handling data correction requests from individuals.

Commonwealth Bank makes the following recommendations:

- We recommend personally identifiable information fields be excluded from write access under the CDR, given the significant security, fraud and privacy risks for consumers. Allowing writing of these fields by ADRs will undermine existing security measures as well as introduce new risks. We recommend that this functionality only be enabled within the CDR once a secure Digital Identity ecosystem is in place to facilitate these changes.
- Any use of write access of consumer information fields in the CDR regime should be voluntary for data holders and should allow data holders to follow existing processes to enable write access requests for consumer information in line with the data holder's risk

appetite, other regulatory obligations (including KYC and AML/CTF), policies and processes.

There are a range of factors that influence the approach a business takes to enabling its customers to update their data, including regulatory obligations, risk appetite, policies and processes. For example, Commonwealth Bank customers are currently able to use online banking or the CommBank App to securely update certain information fields, as there are specific controls in place including multi-factor authentication to reduce the risks of fraud. However there are certain personally identifiable information fields that we do not allow customers to update online in our digital channels to protect customers, as it would create an unacceptable risk of identity takeover or fraud. For these updates we require customers to go to branch or contact the call centre. The CDR should allow data holders to process any write access requests in line with their existing approach for such requests.

We note there may be other data fields that could be enabled for write access, for example, preferences. In these instances, we make the following recommendations:

- At a minimum, an additional validation or authentication step in the consent and authorisation flow be required (e.g. multi-factor authentication)
- Introducing additional controls, such as time delays before any change is given effect, providing data holders, ADRs and the consumer the opportunity to detect fraudulent changes.
- The CDR rules should allow data holders to approach these requests in line with their existing approaches for handling such requests.
- Allowing data holders to apply additional security mechanisms they consider appropriate to protect consumers.

D. Write access – payment initiation

The Issues Paper has identified that a possible use of write access is to enable third parties to initiate payments on behalf of consumers, with the consumer's consent. Commonwealth Bank agrees that write access for payments initiation can bring benefits for consumers. Third party payment initiation has the potential to lessen friction in payments and facilitate a range of use cases.

In recognition of these potential benefits, the payments industry, with the support of the Reserve Bank of Australia, has already commenced developing a solution to enable third parties to initiate payments on behalf of customers, with the customers' consent. NPP Australia (NPPA) is driving this capability in the New Payments Platform (NPP) by requiring NPP participants to develop the Mandated Payments Service (MPS), which will enable customers to give consent to authorised third parties to initiate payments from their bank accounts via the NPP. The planned design of the MPS will enable any third party with an Australian bank account held with an NPP participant bank to send a mandate request (consent request in CDR terms) and initiate a payment request (i.e. write access). This will enable a range of use cases such as subscription type payments, payroll services and e-commerce purchases from a bank account.

All NPP participating financial institutions are required to implement technical upgrades and processes to support the MPS by December 2021. The development of this critical capability will involve a considerable effort to implement, requiring change to existing back office processes and systems. Commonwealth Bank supports the published NPPA Roadmap which mandates this requirement. It is anticipated that financial institutions will begin to roll out services utilising this capability in early 2022. As noted in Section V, Commonwealth Bank recommends that inclusion of write access in the CDR should be deferred until a post-implementation review is conducted of the current CDR regime, which will enable the consideration and design of any future CDR policy to benefit from data-driven findings. This

would allow the CDR to further assess and consider opportunities arising from the NPP third party payments capability under the MPS and whether regulatory intervention is needed in relation to industry led innovations.

For the reasons outlined in Section VI below, it is Commonwealth Bank's view that payment initiation could be best enabled through the MPS which will provide third party write access in a safe, secure and standardised way. As write access for payments initiation will be developed to align as far as possible with the CDR regime, CDR reforms should aim to complement rather than displace the existing regulatory framework of the payments system. We reiterate our earlier recommendations regarding the elements and controls required prior to the introduction of any write access functionality.

Section VI - Linkages and interoperability with existing frameworks and infrastructure

A. Payments systems and infrastructure

The Australian Payments System

The networked nature of the payments system necessitates a high level of co-ordination and co-operation between participants and with regulators. A comprehensive regulatory framework to allocate risks and responsibilities underpins payments infrastructure in Australia, with the ultimate shared objective of maintaining an efficient, secure and resilient payment system. The RBA's Payment System Board primarily regulates the payments system through oversight and strategic direction of industry self-regulation. The policy objectives that have been achieved to date suggest that the current regulatory model is working effectively. In addition to the RBA, APRA and ASIC also have specific responsibilities in relation to participants in the payments system.

Commonwealth Bank appreciates the Inquiry's stated position that *'the CDR regime seeks to build upon and complement the arrangements businesses use'.*[6] Given the complex interplay of multilateral co-ordination required for the clearing and settlement of payments, the CDR regime will need to be integrated with the existing governance framework in a way that does not adversely affect existing arrangements.

Integration of CDR and the payments system

Commonwealth Bank considers that development of payment initiation services within the NPP is sufficient to facilitate write access in the Australian economy, as this is the payment industry's target platform for future innovation and migration of legacy payment streams. In addition to the benefits of the NPP's real time capability and modern infrastructure, the NPP is built on the ISO 20022 message schema which is a globally recognised standard for payments. Further, it is anticipated that some payment rails could be retired in the future as part of a broader rationalisation of payment systems as payment volumes continue to migrate to the NPP.

The NPPA intends to design the MPS to ensure consistency with the CDR standards and requirements for customer consent and data sharing, as well as for the CDR CX requirements and guidelines. The NPPA will also seek to standardise the NPP requirements for Connected Institutions to correspond with ACCC accreditation for the CDR. Commonwealth Bank is committed to working with Treasury, the ACCC, NPPA and the RBA to develop an aligned and complementary process that ensures that entities connecting to the MPS via an ADI are captured under CDR write accreditation.

Deferring the introduction of CDR 'write' access, as recommended in Section V, will assist this process by aligning to the implementation and roll out dates in the NPP Roadmap. Given the potential for regulatory overlap and added complexity to the current framework, the Inquiry will also need to consider the impact and timing of other relevant and concurrent industry and Government work such as the NPP Roadmap, AusPayNet's Future State of Payments industry

[6] Treasury, *Inquiry into the Future Direction of the Consumer Data Right – Issues Paper,* p 6

consultation, ASIC's Review of the ePayments Code and the RBA Review of Retail Payments Regulation.

B. Digital identification and verification processes

There may be benefits for financial institutions and other organisations in collecting consumer identity data through the CDR, for the purposes of 'onboarding' new consumers. These benefits may include the reduction of human error by reducing manual input of key data fields, and an improved customer experience. However, once data is collected, financial institutions have a regulatory obligation to verify that data against *'reliable and independent'*[7] documentation or electronic data, such as a Government database.

Sharing the results of KYC would face impediments were it to be adopted, including:

- That some KYC assessments pre-date improvements in KYC processes, due to the ongoing enhancement of AML-CTF governance (such as the amendment of the Act in 2007);
- Part B KYC requirements are specific to each financial institution and are not standardised across the industry
- Legislative change to allow financial institutions to rely on each other's' KYC assessment.

Given these difficulties, changes to Australia's anti-money laundering and counter-terrorism framework should be not be made through the prism of the CDR. Rather, they should be the result of cooperation with the respective financial crimes regulators in consultation with reporting entities and other organisations captured by the AML-CTF Act.

We also note that the Federal Government has finalised consultation on version 4 of its Trusted Digital Identity Framework (TDIF)[8], and the private sector is developing the Trust ID framework to create a viable digital identity ecosystem in Australia.

Retrofitting the CDR to ensure interoperability with these frameworks will provide limited benefit due to a number of factors.

Firstly, the schemes have different accreditation and ongoing attestation requirements[9]. Providing interoperability between the two ecosystems would either drop the respective security standards for becoming accredited, or significantly increase the costs of accreditation.

Secondly, key concepts regulating the operation of a viable digital identity ecosystem, such as Identity Proofing levels and the roles of attribute provider (as opposed to Identity provider), are absent from the CDR rules and standards. Attempting to incorporate these concepts would require significant redesign of the CDR and we see limited consumer benefits.

Finally, seeking to use the CDR framework as the vehicle for delivering digital identity solutions in the Australian market could significantly slow its rollout, as the CDR regime will likely take

[7] Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007, section 4.2

[8] Digital Transformation Agency, 2020, "Trusted Digital Identity Framework Release 4

[9] For instance, the fourth version of the TDIF requires that all accredited participants produce a Privacy Impact Assessment and Functional Assessment prior to being accredited, and undergo an annual assessment to maintain accreditation (DTA, 2020, "Trusted Digital Identity Framework Release 4", section 2.1)

many years to be mandated across all industries. Australians already have access to digital identity solutions operated by Australia Post and the Federal Government under MyGovID, while Mastercard and Eftpos are piloting solutions.

While the development of digital identity ecosystems are complementary to the spirit and intent of the CDR (in that they allow customers to control and share their data in a secure way), the digital identity frameworks currently being developed are fit for purpose and there is no need for regulatory intervention to support better consumer outcomes.

Section VII - Leveraging CDR infrastructure

Commonwealth Bank recommends increased planning and coordination across the distributed governance structure of the CDR, to support the development and implementation of a robust, secure, and consumer-focused Open Banking regime and ecosystem. While each independent entity is responsible for a different component of the ecosystem, in practice there are occasional overlaps and gaps, creating additional complexity for participants. As discussed in Section V, we recommend accountability for end-to-end security of the CDR ecosystem resides with the regulator, with regular independent security reviews of the ecosystem as standards change and new use cases are introduced. As noted in Section IV, Commonwealth Bank supports the creation of a centralised CDR cyber-security capability across the respective CDR governance entities, which would be accountable for intelligence gathering and coordinating responses to incidents and data breaches.

A. Development of Standards

We recognise the important role of the Data Standards Body in developing common standards for data portability across the economy and information security standards to ensure customer data is held safely from internal and external threats. Commonwealth Bank has worked with the Data Standards Body and industry to help develop standards for a safe and secure Open Banking experience for Australian consumers and businesses. Commonwealth Bank welcomes this opportunity for industries and Government to work together to develop essential standards to uplift performance and security for data sharing across industries and economies.

International developments and the experience of other jurisdictions in implementing their open data agenda provides valuable insights for the design of Australia's data sharing regime. In particular, the technical complexity of a data sharing ecosystem in the UK and Australia is material and cannot be understated. Introducing an Open Banking regime is not only a technology project but also requires large investments in changes to business processes and contribution to an industry-wide standards-setting process. Given the CDR will be rolled out across the Australian economy, Commonwealth Bank recommends a review of the resourcing and operational approach be conducted of Data61 and the ACCC to ensure they are sufficiently resourced to fulfill their critical role in the CDR ecosystem.

Commonwealth Bank continues to support the Government's intentions of embedding learnings from the UK Government's implementation of the Open Banking, whilst recognising there will be some divergences given the differences in Australia's legislative, consumer, regulatory and threat landscape.

We believe there are opportunities to learn from the development of standards for Australia's Open Banking as the CDR is rolled out to new sectors, which are subject to differing regulatory frameworks and have industry-specific approaches that may not be compatible or interoperable. Where feasible, we support greater consistency with existing international standards and industry standards. Where solutions become increasingly bespoke, this creates issues with future extensibility, security and interoperability with other regimes.

Commonwealth Bank recognises the following opportunities for Australia to encourage greater extensibility and interoperability:

- To enable linkages and interoperability with existing domestic and international frameworks and infrastructure, we recommend a reassessment of bespoke Australian CDR security standards to determine which standards would benefit from redesign to achieve greater consistency with existing solutions provided by international standards (such as ISO/IEC 27002 which provides a code of practice for information security controls).
- Assess opportunities for consistency of standards across government departments to rely on commons standards (e.g. API protocols) for data exchange (for example, in 2019 the Comprehensive Credit Reporting authority mandated banks submit batch files for reporting purposes).
- Further enhancements to consent standards (including a consent taxonomy) to introduce optionality for more granular and specific consent. This will provide additional control to consumers over what data they share with ADRs by enabling consumers to only share what is necessary. For example, consumers could specify or filter what data is shared on an account (e.g. only sharing withdrawal transactions on an account, only sharing their postcode rather than their full address, or only sharing transactions that occurred within a particular date range). Standardisation for more granular consents will also be required to enable write access under the CDR regime and is in line with the underlying CDR principle of data minimisation.

Commonwealth Bank also recommends the governing bodies for international industry standards are consulted and directly involved in the development of CDR standards to ensure both best practice for the CDR regime as well as the standardisation required to enable extensibility and interoperability, both nationally and internationally.

B. Accreditation Model

The Open Banking operating model offers strong consumer assurance by being accreditation based. Open Banking provides an opportunity to increase levels of participation through stronger protections for consumers.

We support a robust accreditation process and a tiered accreditation model that reflects the risk profiles associated with expanded read and write activities, without relaxing the existing obligations concerning security, privacy and consumer consent.

The primary consideration of the future CDR regime must be ensuring that consumer trust and confidence in the regime is not reduced through a weakening of the consumer protection mechanisms in the CDR framework. This means ensuring:

1. consumer data is protected by appropriately robust security practices;
2. privacy protections are retained at every step in the process;
3. consumers are appropriately informed and can provide consent in a specific, meaningful and informed manner; and
4. appropriate oversight, monitoring and governance of entities collecting, holding, transmitting and writing CDR data is conducted.

Different accreditation obligations (e.g. security standards, audit requirements) may be useful to distinguish between the different risk profiles associated with various read and write access

activities, and mitigate potential security, fraud and privacy risks arising if the CDR is expanded to include write access (as outlined above in Section V).

Commonwealth Bank recommends the following accreditation requirements for write access be required:

1. Completion of a detailed risk, privacy and cyber security audit, conducted by an auditor who is acknowledged as a trusted auditor by the ACCC. This audit should be refreshed every 12 months.
2. A higher minimum insurance coverage for cyber insurance. Losses could easily exceed the currently required minimum $1M coverage value.
3. Review of an applicant's capital position to ensure that a consumer is reimbursed for any impacts of a data breach, which could easily exceed cyber-insurance coverage.
4. The accredited entity should be subject to ongoing monitoring and auditing by the ACCC to ensure that CDR data is being used appropriately in line with consumer consent and CDR privacy principles.
5. All ecosystem participants should be subject to regular automated conformance testing.

Section VII - Consumer Protection

The objectives of economic value and efficiency will need to be carefully balanced with the need for adequate consumer protection. The CDR, if not developed with the appropriate safeguards, has the potential to increase the exposure of all consumers to breaches of their privacy and fraud. Commonwealth Bank's recommendations regarding consent management design, stringent authentication and verification requirements, and secure technical standards outlined in this submission are aimed at mitigating those risks.

An expansion of write access to payment initiation services poses an additional risk to the stability and integrity of the financial system. The payments industry and the Reserve Bank of Australia's Payment System Board (given its explicit authority for payments system safety and stability) should therefore be engaged in any reforms that may have implications for the broader payments system.

Furthermore, we recommend resources be focused on a comprehensive education program across sectors aimed at raising consumer awareness and understanding of the regime.

Accordingly, Commonwealth Bank continues to take proactive steps to lift the levels of understanding amongst its customers around safe data sharing practices, drawing heavily on existing Government standards as well as lessons from industry best practice.

A. Privacy

To realise the potential economy-wide benefits of the CDR, the regime must engender consumers' confidence and trust. Information security and privacy and security are vital to the regime's success. We have outlined the significant potential privacy risks arising from expansion of the functionality of the CDR as detailed in the Issues Paper, and have provided recommendations on appropriate controls to mitigate these risks (see Sections IV – VII).

Commonwealth Bank supports the robust privacy framework of the CDR and recommends further resources be made available to increase consumer confidence and trust, and drive greater consumer participation. Consumers may not be aware of the distinction between the

robust privacy protections which apply where consumer data is shared through the CDR regime, and the protections available pursuant to the Australian Privacy Principles which apply to personal information shared outside of the regime.

Furthermore, as noted in Section VI, Commonwealth Bank recommends the introduction of a consent taxonomy and the ability to provide more granular and specific consent to provide consumers greater control of the data they share within the CDR regime. This will also provide greater privacy protections to consumers by enabling only essential data to be shared (e.g. only sharing withdrawal transactions on an account, only sharing their postcode rather than their full address, or only sharing transactions that occurred within a particular date range) as outlined above in Section VII.

B. Vulnerability

The growing digital economy and rise of data portability schemes presents new challenges and requires a reframing and reconsideration of who is considered vulnerable in the context of the CDR regime. The increasing prevalence of digitisation and open data raises a broad range of issues for consumers including access to technology; data empowerment; bias; data literacy; and data ethics.

These issues will exacerbate existing difficulties faced by vulnerable consumers and create new challenges for this broad segment. These issues are expected to intensify with the significantly increased online activity and economic uncertainty associated with the COVID-19 pandemic. Furthermore, there may be additional, yet to be assessed, risks to a broader set of vulnerable cohorts than traditionally considered, such as people who choose not to participate in data sharing regimes, and people with low financial literacy who are highly engaged users of digital platforms.

As digital literacy and access to technology are pre-requisites for consumers to benefit from the CDR, vulnerable groups will face the same structural barriers that are associated with any digital financial service. These include access to supporting infrastructure and internet access in regional and remote areas, and the lower access to and use of smartphones by older consumers, people on low incomes, people experiencing (or at risk of) homelessness, people with disability, and consumers with low English proficiency.

In relation to payments, specific issues have arisen in terms of accessibility of technology for consumers with disabilities. The existing work by the payments industry in this area, together with the Australian Payments Council's Strategic Agenda work on financial inclusion and accessibility of digital payments will be relevant to any data-based reforms regarding payment initiation services.

In general, vulnerable consumers face a number of risks of disadvantage and discrimination including greater susceptibility to coerced or uninformed consent, fraud, predatory lending, elder abuse and other unethical conduct, mis-selling or denial of services. Greater access to consumer data is likely to increase the risk of exploitation if proper measures are not put in place.

However, inversely, the CDR and Open Banking also has the potential to play a valuable role in helping vulnerable consumers manage their financial data and protect their financial wellbeing. For example, making consumer data available to trusted third parties to monitor accounts where a consumer or their personal legal representative may have concerns about financial abuse by another person with access to the consumer's accounts. These types of

ancillary consumer protection may prove a compelling use case to increase rate of customer adoption and of community advocacy for Open Banking. Commonwealth Bank is committed to working with the Inquiry to ensure that the design of the CDR is inclusive of the needs and choices of all consumers and specifically provides benefits for traditionally vulnerable consumers.

Closing Remarks

Australians and Australian businesses are facing unprecedented times as we grapple with the impacts of the COVID-19 pandemic. As Australia's largest retail bank we have a vital role to play in helping support our customers and the Australian community, and we have a unique privilege and responsibility to serve our customers during this experience in their lives. As a sector, we are diverting significant resources to prioritise initiatives that support our customers and the Australian economy towards a path to recovery. The financial impacts of COVID-19 to our customers will be varied and long lasting and it is important that we consider any further introduction of scope into the CDR regime through this prism. Further, there are a number of particular risks that must be carefully managed to ensure the integrity and security of the ecosystem, and to ensure consumer protections are embedded into the design of the CDR. As such, we recommend the Inquiry has regard to the need to bed down and resolve issues associated with Open Banking policy changes and consider practical timelines for any potential expansions of the CDR raised in the Issues Paper given the significant lead times for implementing technology reforms of this kind.

Commonwealth Bank appreciates the opportunity for continued dialogue on the future of the CDR.