Statutory Review of the Consumer Data Right: Issues paper

Submission by:

Friday 10th June, 2022

BASIQ

Basiq (ABN: 95 616 592 011)
7 Raglan Street
Manly, NSW 2095

Table of Contents

Summary	**4**
1. Complex Accreditation	**6**
2. Reciprocity obligations are too onerous	**8**
3. Improve Industry Engagement	**9**
4. Define KPIs to measure success	**11**
5. Select Industries that will deliver greatest impact	**12**
6. Fast-tracking the roll-out of “write” services	**13**
7. Reduce the cost of Data Holder Implementation	**15**
8. Quality of CDR Data is unknown	**16**
9. Consumer onboarding is too complicated	**18**
10. Inconsistent onboarding between Data Holders	**20**
11. Open Banking authorisation has limitations	**21**
12. CDR should be extended to other data sources	**23**

Background

The Australian Government has initiated an ambitious program called the Consumer Data Rights (CDR) which seeks to level the playing field and increase competition within industries by enforcing organisations to share consumer consented data they hold on consumers. The first target industry was the Banking sector under a program called “Open Banking”, with other industries such as energy, telecommunications and insurance to follow.

Consumer Data Right (CDR)		**Open Banking**
Provides the legal framework, accreditation, and specific rules around the sharing and handling of consumer data. These rules are industry agnostic.	→	Defines a set of API specifications and requirements that “Banks” (ADIs) must adhere to in order to securely share their consumer data with accredited 3rd parties

With the first release of Open Banking APIs dating as far back as July 2019 (almost 3 years ago) we examine where we are today. This document examines some of the the benefits and current draw-backs that we believe are holding back the adoption of Open Banking, and provides suggestions on how to make the program successful.

Summary

Problem Statements	Resistance to Adoption	Impact on Use Case
1. Complex Accreditation It is expensive to implement, lengthy to acquire and complicated to interpret the rules.	High	Medium
2. Reciprocity obligations are too onerous Current reciprocity discourages non-bank creditors from participating.	High	High
3. Improve Industry Engagement Key stakeholders should be more actively engaged to ensure appropriate feedback is being considered.	Medium	Medium
4. Define KPIs to measure success The current KPIs are leading us to incorrect measures of success. We should define KPIs that measure true success of the program.	Low	Medium
5. Select Industries that will deliver greatest impact Careful consideration and better industry involvement should consider industries where greatest impact can be delivered.	Medium	Medium
6. Fast-tracking the roll-out of “write” services Ability to deliver true value of CDR will be stalled until write services are in place.	Low	Medium

Problem Statements	Resistance to Adoption	Impact on Use Case
7. Reduce the cost of Data Holder Implementation Data Holder solutions are expensive to implement.	Medium	Low
8. Quality of CDR Data is unknown CDR does not provide any guarantees nor is there any form of testing on quality of the data.	High	High
9. Consumer onboarding is too complicated Current Open Banking onboarding is too complicated for consumers and introduces too much friction.	High	High
10. Inconsistent onboarding between Data Holders Inconsistent implementations between Data Holders introduce onboarding friction for consumers.	Low	Medium
11. Open Banking authorisation has limitations Consumers have the ability to be selective on what accounts they choose to share.	High	High
12. CDR should be extended to other data sources Accredited parties should be allowed to demonstrate CDR data handling across non-CDR data sources.	Low	Low

1. Complex Accreditation

There are two general forms of participation within Open Banking, you are either a Data Holder (DH) i.e. you hold consumer data and are required to expose the data you hold on consumers; or you are a Data Recipient (DR) i.e. you are seeking to read consumer data from a DH in order to deliver some sort of service to the end consumer.

To be able to read data from a DH (i.e. *to be able to call an API from a bank*) the DR must undergo a complex accreditation process. This process typically requires the DR to hire an external consultant to help them provide the appropriate material for submission to the accreditation authorities, at which point upon approval, they will be issued with the appropriate tools to begin their development (or make their first Open Banking API call).

On 5 October 2021 the Government released new models in an attempt to reduce the friction associated with the accreditation process. Although these models have provided greater options, we feel that they have still not solved the underlying problems that were originally raised during the proposal phase. As it stands now, the accreditations are still considered to be **expensive to implement, lengthy to acquire and complicated to interpret the rules associated with them**.

We believe that the reason for this is the failure to put the practical adoption requirements (*faster onboarding*) and reducing the barriers to the program ahead of the principles concerning liability (i.e. who do we hold accountable if things go wrong). As a result, we two groups of accreditation as follows:

- The Accredited Data Recipient (ADR) is liable; these models include full ADR accreditation and Sponsor Affiliate Accreditation. These are more difficult to acquire and have the greatest penalty i.e. you have to spend time and money to get accreditation and are penalised by holding the greatest liability.

- The DR is not liable; these models include Principle Representative. This model is easiest to acquire, but requires an ADR to carry the liability on their behalf - meaning if anything goes wrong the ADR will be held accountable.

The range of models that have been offered simply provide an illusion of optionality, because they do not take into consideration the complexity of integrating with the Open Banking specification. Due to these complexities any party seeking to use Open Banking data will most likely engage with a 3rd party organisation to provide them access services, as these organisations have done the hard work of connecting to the DH and providing core services to make Open Banking easy to consume. As a result, other than the benefit of end consumers being able to easily share Open Banking data to their Trusted Advisers, the real number of accreditation options is significantly reduced to the following scenarios:

- Either the 3rd party takes on the liability on behalf of the recipient looking to consume the data;
- Or the recipient is required to spend time and costs to gain full ADR accreditation or Sponsor Affiliate accreditation.

Our recommendation is to simplify the accreditation tiers by doing the following:

- Have one accreditation: (full) ADR accreditation. This accreditation enables parties to directly interact with Data Holders and the ACCC register. These organisations are required to ensure they have met all data handling requirements and provide the tools that conform to the handling of consumer data.

- Shared liability model. Any organisation that uses ADR services will be held accountable to conforming to the same data handling standards as the ADR, with the ADR responsible for providing data governance assistance, training and tools to potential participants. This will force a model by which ADRs will be providing the services around data governance and consent management to non accredited recipients. However, in the event of a data breach or mishandling of data, the party that violated these issues should be held accountable - not the ADR (unless they were in breach).

By simplifying the accreditation models, and sharing the liability we believe that the adoption of Open Banking will be significantly accelerated as ADRs will be encouraged to provide the tooling around data handling, consent management and general data governance. This will enable Data Recipients to get to market faster, without the concerns of accreditation hanging over their heads.

2. Reciprocity obligations are too onerous

There is a provision within the CDR rules that states (in over-simplified terms) that, if you become an accredited recipient of CDR data and your business happens to provide similar products to that of the data you are consuming, that you will then be required to also expose the data that you have/hold on your consumers.

In practical terms this means that if a non-bank lender becomes accredited, and consumes data from a bank (i.e. calls their APIs) they will also be required to become a Data Holder and develop / provide a set of APIs that other parties can call to access their consumer data.

We understand that the intention behind this was to encourage more participants to also share the data that they hold on consumers, and have more API services / data accessible in the ecosystem. Unfortunately this has simply had the opposite effect, and has discouraged companies that would be beneficiaries of Open Banking data to avoid the adoption, or try and find loop-holes by seeking non-accreditation access such as via the Principle Representative (PR) model to circumvent this requirement. As stated earlier, the PR model places the liability on the ADR providing the services, to which they are just as discouraged to offer given they carry the liability if things go wrong.

The other danger of this statement is that it does not acknowledge the shape or size of the company that would be held liable as part of the reciprocity clause. Meaning that a small fintech which may have just launched with no revenue would also be held accountable to meet the requirements of becoming a data holder (before they can even use Open Banking services). This cost would simply be too great for them to bear and would provide absolutely no justification for the usage of Open Banking services.

Our recommendation is to simply remove this from the CDR rules to reduce the friction, and increase the adoption of Open Banking. The process of encouraging non-bank lenders to participate can be handled as a separate exercise as the Government has already commenced their investigation into.

Furthermore, the reciprocal sharing of data for all recipients could always be revisited once the CDR framework has been fully established.

3. Improve Industry Engagement

When driving initiatives like CDR and Open Banking it is really important to have the right representatives and contributors involved to provide reasonable feedback and to help ensure the program is heading toward the right path. The Government has demonstrated through action their willingness to engage with the wider fintech community through various channels and panels, however we feel that the participation of some of the key stakeholders should be re-evaluated to ensure that the Government is gaining appropriate feedback from organisations that have first hand experience with the consuming and provision of financial data services within the industry.

Engage with experienced data aggregators

To do this, the Government must ensure that it acknowledges the existence of data aggregation services (that rely on technology such as “screen-scraping”) and that it sees organisations that use or provide these services as one of the most valuable sources of information. As these companies are most familiar with:

- The data that is being offered by Open Banking, and its limitations.
- The practical usage of this data to deliver value to consumers.
- The buying / deployment process required to adopt data aggregation services.
- The deficiencies in the data, and how it can be improved.
- The deficiencies with “screen-scraping” that should be resolved with open banking.

Furthermore, these organisations are also most likely to promote Open Banking services to the industry and their consumers are most likely to adopt Open Banking given they already adopt scraping methods.

Unfortunately, companies such as Yodlee, Illion and Basiq that have been providing data aggregation services to millions of customers and work with hundreds of Fintechs in Australia are insufficiently engaged, and in some circumstances are not even present in key discussions. This is a completely lost opportunity which leads us to a path of “reinventing the wheel” or worse a path - where we make avoidable mistakes.

We would also encourage the Government to carefully consider taking advice from organisations that have: recently formed; have few Fintech customers; or have never provided financial data services in any production environment.

Basiq has been providing data aggregation services in Australia since 2017, has enabled over 1.5M Australians to share their banking data, and services over 150 Fintech customers. We can attest to the differences behind making a theoretical suggestion and a practical one. The nuances and experience of companies like Basiq are imperative and we would encourage the Government to be more inclusive in ensuring that they extract as much value from companies that have experience providing services in this space, and be wary of ones just starting out with little to no experience.

Engage with experienced Fintechs

Similar to the point raised earlier in regards to working closer with experienced data aggregators, we would equally encourage the Government to work closer with Fintech organisations that are currently consuming financial and banking data via APIs using data aggregators. These Fintech organisations provide valuable insights as they have worked for years with this data (which is the same data that Open Banking makes available). Furthermore, these organisations can also provide input into the following:

- How to optimise the user-experience when introducing bank connectivity functionality
- Provide a detailed explanation of how this data is being used to deliver value to consumers
- Identify the limitations in the data that may be prohibiting them from innovating
- Provide a great representation of consumer needs and behaviours

Although there are some Fintechs that are participating and providing input to the roll out of Open Banking, we found that larger organisations that rely heavily on this data, have hundreds of thousands of active users, and have been using data aggregation services for +5 years, are not being consulted about their experiences.

It is also important to note that these organisations (similar to Data Holders) will be substantially impacted when migrating over to data governed by CDR rules and made available via Open Banking pipes. These impacts include rules around consent handling, the lack of UX experience control (due to prescribed guidelines) and data governance rules. These are important factors that need to be equally considered to ensure a smooth transition to Open Banking technology solutions.

This is genuinely a lost opportunity, as these customers will also likely become the largest users of Open Banking services. We have also found that due to the lack of involvement from these organisations, their view of Open Banking is sceptical and the need to fix or change to something, which from their point of view doesn't feel broken, will make it harder to get them to adopt Open Banking.

4. Define KPIs to measure success

We have seen that the Government has been using KPIs such as the number of accredited parties and number of data holders participating in the program. We consider these as secondary metrics and would urge the Government to consider changing these to place the **number of active consumers** sharing data (within a month) to be the primary metric of the program. This is critical, and will ensure that all of our efforts are aligned to the successful outcomes of delivering value to consumers rather than outputs of the program.

Defining this metric as the key measure of success will ensure that everyone is aligned and focused on increasing adoption. It will ensure that the adoption is driven by making the data easily accessible and reliable for Fintechs, who will ultimately deliver value to consumers.

With the KPIs that have been communicated to date, one could argue that the Government has already reached complete success with the rollout of the CDR program as the number of data holders and coverage of Australians (as defined by household deposits) has already been met. However, the adoption is still incredibly low, and measuring the number of accredited parties is equally irrelevant if these parties are not delivering any consumer value, or have not delivered the ability of Open Banking services to consumers.

5. Select Industries that will deliver greatest impact

We would urge the Government to carefully consider the target industries for the roll out of the CDR program, to ensure that it will have maximum impact on innovation and delivery of valued services to consumers. For example, instead of the upcoming release of Energy (and Telecommunications to follow), we believe that other industries such as Superannuation and Government services would have been more appropriate.

This recommendation is based on feedback from our Fintech customers, where they have expressed a strong desire to access data from these segments to drive greater efficiencies in the delivery of their services and provide greater consumer value. For instance, if these services were available now (or next), Fintechs would be able to:

- Automate the process of determining an individual's income (so no more payslips)
- Provide greater insights and control into their future investments
- Provide identity services that would help with consumer onboarding and regulation
- Provide deeper insights of Government assistance services
- Provide new attributes that could be used for more efficient credit risk modelling

We are aware that the Government has also initiated a consultation into the non-bank lender sector. When asked as to the reasons why this was selected, we were informed that it would enable businesses to provide a more complete picture of an individual's finances. We can confirm having serviced over 150 Fintechs, of which the majority provide lending services, providing access to data from Superannuation and Government services would provide more value in getting a complete picture of an individual's finances.

Basiq has been offering data services that provide connectivity to Banks and non-bank lenders for many years, and can confirm that the usage of non-bank lender data is very low. Furthermore, most of the scenarios which Fintechs think may be solved by adding non-bank lenders, can already be solved with banking data alone (e.g. identifying income and liabilities through transaction data / records).

Our recommendation is to carefully consider industries which will provide the greatest impact to innovation. A good framework for determining this is to consider existing data exchange practices, e.g. the exchange of bank statements with lenders, real-estate agents and other services has been a common practice - highlighting the general need for this data. Taking a similar approach and looking at what data consumers need to provide in exchange for a service should be a key decision in determining the industries the Government seeks as it rolls out the CDR.

6. Fast-tracking the roll-out of “write” services

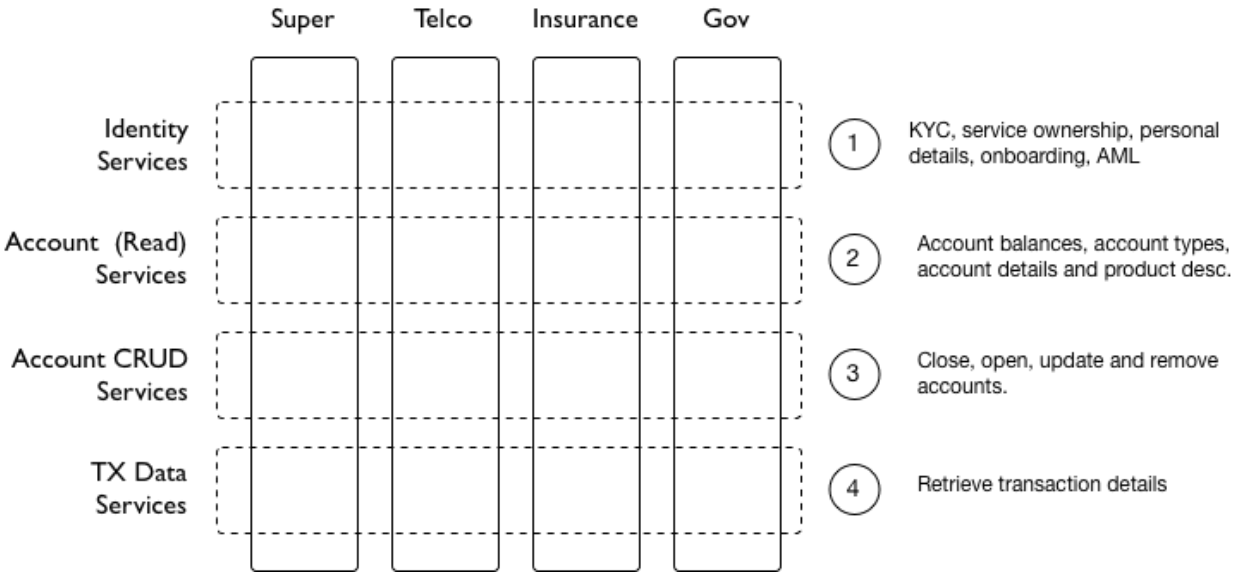
One of the greatest missed opportunities of the CDR program was not incorporating write services as part of the roll-out. Write services provide the ability to “action” changes to consumer’s data (e.g. updating account or personal details, closing / opening accounts, upgrading / downgrading services, paying merchants, or receiving funds from a merchant).

As a result, we believe that the CDR program at best will be able to provide insight services to consumers, such as the ability to see all their bank balances in one place with no ability to take any action on this. This, in the end, becomes as useless as a budgeting spreadsheet - where the data and insights are present with no ability to take action.

Moving from industry-to-industry focussing just on read access will make it harder to come back to these sectors and enforce action services. Secondly, write services will likely have an impact on the data services which have been prescribed - forcing some of them to change in order to make the process of read / write more integrated.

One recommended approach is to consider amending the program to incorporate horizontal slices across multiple industries simultaneously to provide the following functional services:

- Identity services - the ability to authenticate and return back identity data
- Ability to acquire account level data
- Account management services - Create, Read, Update, Delete (CRUD)
- Ability to acquire transaction level data



One of the benefits of taking this approach is that it would provide the greatest value across multiple sectors simultaneously, having the biggest impact to the Australian economy. For example, rolling out identity services across multiple industries would enable the process of KYC, customer onboarding and capture of personal details to be solved for any software product (regardless of the industry it operates in). This would also encourage a wider adoption of CDR services across the entire development sector, substantially increasing adoption and usage of CDR services.

This approach could be further enhanced by ensuring that some sort of real-time payment infrastructure service is also being delivered simultaneously (e.g. NPP or action initiation services). The combination of data, account and payment services would provide the richest level of services across multiple industries, and would create an incredibly rich set of services and segments not available in any other region in the world, making Australia truly stand out as an innovator.

7. Reduce the cost of Data Holder Implementation

As the Government looks to roll out the CDR program across a number of industry sectors, one of the things that may become prohibitive for these sectors to participate in is the implementation cost of a Data Holder solution. The Data Holder solution would be considered a significant investment for most small to medium sized businesses. These complex solutions require a lot of design work, development and ongoing fees to keep the platform up to date and ensure that it is regularly updated to meet the latest security requirements.

To make it easier for these businesses to participate in the program, we recommend that the Government invests in a reference implementation project that provides an out-of-the-box solution for organisations to meet their data holder requirements. This solution could be open sourced to ensure that organisations are able to assist each other, and to keep the code up to date with ongoing requirements.

Providing a solution like this would enable data holders to drastically speed up the implementation of data holder api services, and would also further help with the following:

- Improving on the reliability of data holder api services
- Ensure that outputted data complies with CDR rules and respective industry standards
- Ensure the data is being managed in a secure manner
- Speed the roll out of CDR changes to data holders e.g. if the entire banking industry used a reference solution - the roll out of joint account changes could have been more easily rolled out

8. Quality of CDR Data is unknown

One of the biggest unknowns with Open Banking is the quality or completeness of data that comes out of it. Unfortunately the Conformance Testing that is performed to validate whether a Data Holder has met their obligations, **does not test the quality of the financial data**. As a result, nobody can confidently measure the quality of the data, nor guarantee that the data that is supplied via the Open Banking APIs is complete.

As the main purpose of the Open Banking services currently is to supply data, it is essential that Data Recipients are able to safely rely on the data that is produced. Without providing guarantees, it presents a number of issues within the industry:

- Fintechs are reluctant to switch from services such as “scraping” to “open banking” as they may get more data from the former given consumers can selectively omit some data that may not be as flattering

- If the data is incorrect or in a poor state, it may encourage lenders to issue loans which should not be otherwise given; or restrict credit to applicants who may be eligible

- May encourage consumers to act on insights derived from data that is incorrect

We are cautious of encouraging our customers to make any transition to Open Banking until we have confidently tested the quality and completeness of the data that is produced via the APIs. Our concerns that the data may be invalid are as follows:

- There was no testing of the data that is output by the Data Holders.

- We discovered that some institutions do not output data for all accounts (e.g. some data may reside in an older database which the Data Holder has not integrated with the Open Banking services).

- We discovered inconsistencies in the data within the same institution where depending on the type of account / product the data would vary e.g. some credit card accounts may include balances while other similar accounts/products excluded this attribute.

- We discovered that essential attributes such as account number and details were missing for accounts. Note that this breaks many payment use cases that rely on these attributes to capture account details; prove account ownership and set up direct debit payments.

- Many of the institutions are still not supplying specific account types which may be of use to Data Recipients - the list is published on the CDR website - however please note that these are the only ones which have been reported and in reality there may be more which we are not aware of.

https://www.cdr.gov.au/for-providers/rectification-schedules/rectification-schedule-active-data-holders-gaps

- Some banks did not provide access to pending transactions (this also occurs within the same bank across multiple accounts / products).

One of the reasons for the poor data quality (we believe) is that when the data holders implemented their solution they:

- Focused on the timeline to meet their regulatory requirements - which does not test the data and only validates that they have produced the APIs to specification;

- For many of the banks there is no central account and transaction table from which to pull data - instead this data is scattered across their enterprise - and some of it may have been missed or is difficult to acquire.

- Some of the banks integrated the Open Banking APIs directly with their core database - rather than the refined data that drives their existing internet banking portals.

  Note that the internet banking portals have been used for +20 years, and are tested almost daily by the account holders (simply through the act of logging in to their banking portal and seeing their accounts, balances and transactions). Whereas core banking systems that store lower levels of data may not have the same completeness of testing as consumers see.

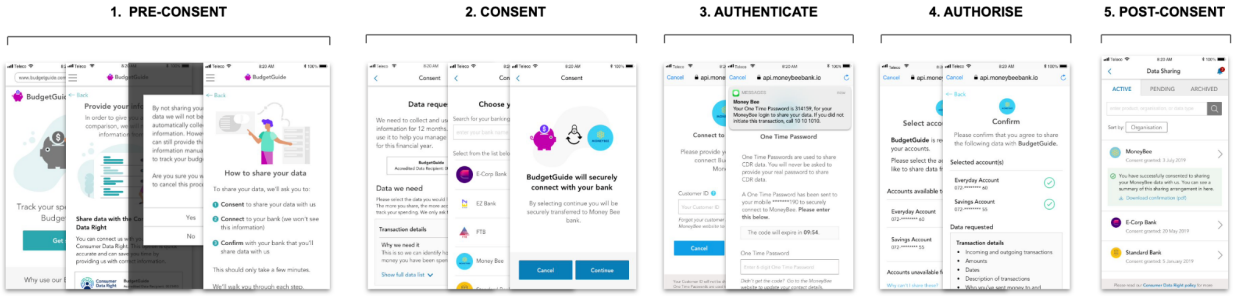
As a result of this, “screen-scraping” is the only method at present that provides a reliable stream of data - i.e. it guarantees that the data that the consumer sees via their internet banking portal, is the same data that is outputted via aggregators APIs. However, Open Banking does not provide any guarantees that the data is the same. This is a very serious issue which we believe should be urgently addressed.

We recommend that the Government increases the requirements of the Conformance Test Suite that requires Banks to prove that they have tested the completeness and correctness of the data that is provided via the Data Holder API services. This could be taken further, by ensuring that there is a public register that outlines what data can be expected and identifies the quality of the output.

9. Consumer onboarding is too complicated

The present CDR CX Guidelines provide a detailed description of best practices and guidelines of the CDR rules and how they could be interpreted. We believe that the CDR CX team has done an amazing job with these recommendations, however we are generally concerned with the number of steps required to complete the flow and the cognitive overload presented to the consumer as a result of the onboarding process.

The current CDR CX recommendations organise the process of linking a bank account in the following steps: pre-consent, consent, authentication and authorisation. These steps in total include approximately 11 UI screens - that could possibly be presented to the consumer. These screens also don't take into account that the consumer may also be performing the linking of their bank account during an application's own sign-up process which will also have its own UI screens (e.g. user registration, email verification, KYC checks and more).



The more screens that are present generally increases the likelihood that a user will abort signing up to a Data Recipients (Fintechs) service as it may feel "too hard", "too complex" or the value is diminished with the time it takes to onboard with an app. We believe that this complexity discourages Fintechs from considering Open Banking due to the following reasons:

- They have significantly less control over the UX requirement than that of services like "screen scraping" where the Fintech is able to control the entire user experience.

- The chance of drop-offs is a significant risk for Fintechs which after spending their own time and resources to convince users to try out their app may lead to users abandoning their service.

- The more screens that are available, especially that are outside of the Fintechs control also introduces potential for errors e.g. a bank may have a javascript bug on their website that prevents users from progressing - this would have a direct impact on the Fintech's own application preventing the user from being able to return back to the Fintech app.

Our recommendation is that the CX team gives greater consideration to the Fintech's requirements, and considers removing or reducing the number of screens required to complete the consent process. One suggestion would be to reduce the number of screens involved on the data holder's end, and to see if there are other ways of reducing the number of screens required on the data recipient's end.

10. Inconsistent onboarding between Data Holders

There was a lot of effort to standardise the technical implementation of the assets produced as part of the CDR program. This includes onboarding flows, api services and other mechanics required to consume API data.

One of the observations which we have made is the level of inconsistencies between the various data holder solutions when it comes to users completing the authorisation flow (e.g. a single user wanting to link their Westpac and CBA account will be required to go through drastically different flows). For instance, via Westpac, the user is able to perform the authorisation via the redirected web site, whereas via CBA, the user is required to install the CBA app, then navigate between the CBA app and the Fintech app to successfully complete the authorisation process.

Note this means that if a user attempts to use a Fintech app on a new device where they do not have a CBA app installed, they will be prevented from being able to successfully link up their CBA account on that device.

Additionally, the messaging is also inconsistent between the various Data Holders, further complicating the onboarding process and the user experience as a whole (in addition to the aforementioned issue relating to too many screens). As a result this increases the potential for user drop-offs and reduces the success of a user completing the process of linking up their bank accounts.

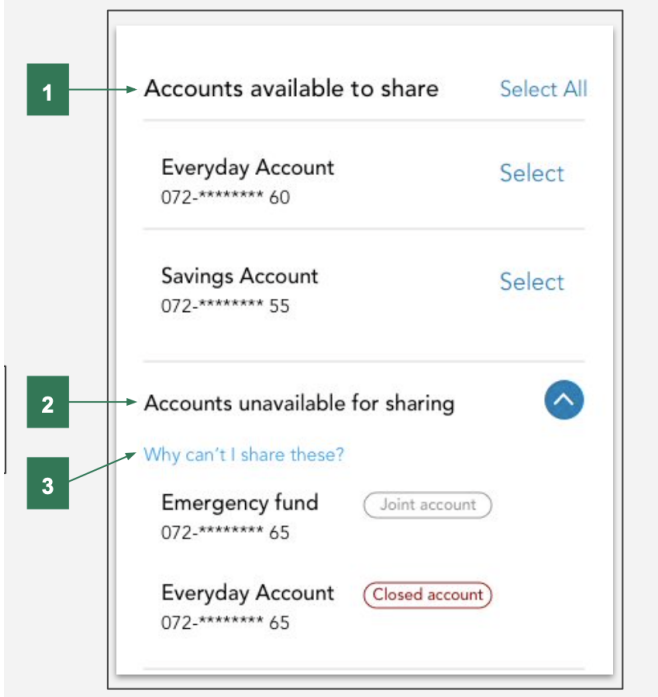
We recommend that the CDR program standardise the flow across the data holders so there is a single consistent experience across the data holders. This will provide a seamless experience for the users and will ensure that users are familiar with the process of onboarding across the various institutions.

11. Open Banking authorisation has limitations

The design of the CDR program alongside the CDR CX requirements puts the consumer in direct control of their data. The consumers are informed of the data they are sharing and have varying levels of controls as to what data they wish to share, and for what intended purposes.

Although the CDR program has done a great job of putting consumers in full control of their data, we believe that the fine balance between practicality and control is unbalanced. So much so that with the current CDR implementation the consumer has the ability to break any use cases where Open Banking is being used.

The main issue stems from being able to provide the consumer with the ability to select the specific accounts they wish to share with the Fintech provider. This occurs once a consumer has successfully authenticated with the data holder (i.e. has passed the login screen) and is then asked by the data holder (the bank) which accounts they wish to share. This screen is the main problem, because without knowing the full inner workings of the Fintech application, the consumer is uneducated as to which accounts they should/shouldn't share. Furthermore, the consumer may also consciously elect not to share specific accounts when applying for a loan to paint a better picture of their personal finances.



Use Cases	User Selection	Failure
Capture account details to set up direct debit payments	● Mortgage Account ● Term Deposit Account	The user selects an account type from where direct debits cannot be performed. This would lead to a failure by the Fintech app to be able to execute the use case.
Acquire account and transaction data from consumers for purpose of making a credit decision	● Keycard (selects) ● Credit Card (ommits) ● Personal Loan (ommits)	The user has selected their keycard only and has intentionally omitted their credit card and personal loan accounts. The lender is not aware of this, and only receives keycard data - and uses this to make a lending decision. The data looks “ok” and the consumer is issued a loan. Had the consumer shared their other accounts the lender may not have given them a loan.
Consumers use a budgeting app (PFM app) to track their spending.	● Mortgage ● Term Deposit ● Savings Account	The PFM application reports incorrect data to the consumer as it doesn’t have the complete picture. The app fails to deliver value to the consumer, and the consumer deletes the app. The Fintech loses the consumer due to a poor experience.

Using other methods such as “screen scraping”, the authorisation flow **does not** enable the consumer to select which data to share as it introduces the ability for consumers to make a mistake (which is a design 101 of what not to do).

Instead, the recommended approach should work with the Data Recipient sending a request to the Data Holder of what data they require as they know best how their application works. The Data Holder then presents the request to the consumer at which point they are given the option to provide a Yes / No answer. If accepted, the Data Recipient will be granted access to the accounts they require.

This approach still ensures that the consumer is informed and in control, and ensures the consumer does not break the function of the Data Recipient. If the consumer does not feel comfortable with the sharing of the data they can simply decline the request.

12. CDR should be extended to other data sources

The CDR program provides a great structure that enforces good principles around the handling of consumer data and capture and management of consent to access data. Unfortunately these rules only apply to data that is accessed through participating CDR regimes.

We believe that this is a missed opportunity and would encourage the Government to consider enabling voluntary parties to use their CDR accreditation to communicate a standardised approach to handling of data to assets outside of participating industries. For instance, if a company has adopted CDR as a standard way for managing all data through their platform (e.g. open banking or other data not part of CDR), the accredited party should be able to use their badge to indicate that they have been accredited and that they have adapted practices to meet the standards set out by the CDR program.

Enabling this would help speed up the adoption of the CDR program as it would encourage industries to adapt the same Data Governance and consent management principles even if they are not part of a CDR participating industry.