21 October 2019

Caroline Atkins & Kathryn Armitage
Partners
Public Law, Maddocks
Level 1, Maddocks House
40 Macquarie Street
Barton ACT 2600
by email: cdrpia@maddocks.com.au

Dear Ms Atkins and Ms Armitage

Consumer Data Right Regime Privacy Impact Assessment

Thank you for the opportunity to comment on Consumer Data Right (**CDR**) regime Privacy Impact Assessment. The Financial Rights Legal Centre (**Financial Rights**) has previously supported the need for an independent privacy assessment on the CDR and appreciate Treasury empowering and resourcing Maddocks to undertake this important task.

We believe that this draft PIA has undertaken a thorough assessment of the potential risks arising from the CDR legislation and has identified a series of new, previously unidentified risks that have the potential to have serious impacts upon consumers. This is the value of an independent Privacy Impact Assessment.

We also note that the PIA does not evaluate the risks on a risk and likelihood matrix. This is a positive step. Where a risk has been identified - that risk should be mitigated.

We believe that this draft PIA has made a series of sensible recommendations within the remit and scope that they have before them and we support Treasury, government and the regulators of the CDR acting swiftly to implement them to ensure that consumers are provided with further protections before the launch of open banking. At a number of points below we make the case for the PIA to make further recommendations which we believe should be included. These include:

- Ensuring that changes to CDR standards and Guidelines trigger a supplementary PIA;
- Extended protections for consumers who provide CDR data to unaccredited third parties;
- Requiring guidelines be binding and enforceable

- Requiring Accredited Recipients (and Data Holders) to delete or de-identify third party information after it is used or that this data be reconfigured to maintain the utility of such data but remove the risks.

Recommendation 1 – Further Updates to this PIA

The PIA of the CDR regime must, by its very nature, be a living document– updated regularly as the CDR develops and expands its coverage of sectors. We therefore support Recommendation 1.

The criteria triggering a further PIA are generally comprehensive and should cover most areas of core concern. For example, if there were to be a change in the Rules to allow direct marketing or the on-selling of data this would invoke an update under the criterion "any other change to the legislative framework (including the Draft Rules) that would impact on the application of the Privacy Safeguards and or the APPs.

If new legislation is introduced that amends, expands or detracts from the current legislative framework a supplementary PIA would be triggered. We note on this point that *Treasury Laws Amendment (2019 Measures No. 2) Bill 2019* passed parliament yesterday introducing a requirement to delete CDR data in response to request from CDR consumer. The current PIA should by rights consider the positive impacts of this new protection. If it does not, there should be a supplementary PIA.

One area that is less clear is whether any changes to the Data Standards and CX Guidelines would trigger an update. Many of these standards and guidelines will have a direct impact upon the real world privacy practices of Data Recipients and Holders as well as the privacy rights of consumers. Many of the issues that arise are critically important with respect to the enlivenment of the CDR legislation and rules and their impact on privacy. These can include what information is prioritised on the first screen of a consent page; whether Data Holders can introduce the concept of a "temporary stop" on deleting data; or providing consent management paper trials for consumers and lawyers to access when things go wrong.

The standards will be in place in time but there is high likelihood that they will be changed over time.

If it is intended that a substantive change to the standards and guidelines would trigger a reconsideration of the PIA – then this should be stated explicitly.

If changes to standards and guidelines are not currently intended to lead to a reconsideration of the PIA – we believe that they should.

Recommendation 2 – Further guidance on the operation of the CDR regime

Financial Rights strongly supports the development and provision of guidance on when protections in the CDR legislative framework will apply to particular data, when entities will be a Data Holder; and when Data will be defined as CDR Data.

As we have argued in multiple submissions what has been developed by Treasury is incredibly complex, varied and inconsistent. Because CDR is incredibly complex, varied and inconsistent

this ultimately disempowers consumers who will struggle to understand what they can do and what their rights are when things inevitably go wrong.

This complexity has been well established by Maddocks in this draft PIA and we applaud Maddocks' attempt at distilling some of this complexity down in the Diagrams of Information Flows as an attempt to explain the issues in a simple form.

Having said that a consumer is still unlikely to understand and engage with these disclosure documents. As ASIC have just reported

> *Disclosure cannot solve complexity that is inherent in products and processes. Simplifying disclosure, for example, does not reduce the underlying complexity in financial products and services. Nor does it ease the contextual and emotional dimensions of financial decision making, both at the point of purchase and over time.*[1]

The same sentiments apply to the Consumer Data Right. No amount of information provision will solve the problems arising out of the complexity identified by Maddocks, nor will consumer education mitigate against poor consumer outcomes in this space.

This is not to say that we should not provide disclosure documents to consumers and attempt to make it easier for them when things do go wrong. There remains significant utility in the development and distribution of these documents for consumers and their representatives. They will however do little to protect consumers in the first place.

The onus to ensure consumers are not exploited should not fall on the consumers themselves. Personal responsibility can only go so far when there are very real financial incentives motivating Data Recipients and Data Holders to direct consumer decision making in self-serving directions. Complexity is one key tool used by firms to undermine rational consumer decision making – a lesson that is clear in the insurance space for example.

Consequently it is incumbent on government and regulators to get CDR consumer protections this right by building privacy by design into every aspect of the CDR and implementing rules and regulations that will mitigate against consumer harms This will involve preventing Data Holders and Recipients from doing certain things and acting in particular ways. Regulatory intervention will be the only way to prevent the harm that is likely to arise in the misuse and exploitation that will arise in open banking and other sectors impacted by the CDR.

Recommendation 3 – Further guidance of the Draft Rules

Financial Rights strongly supports the six recommendations that make up Recommendation 3 as positive steps to mitigate consumer harm. We wish to however provide further comment on recommendation 3.3.

[1] Page 5, ASIC Rep 632: Disclosure: Why it shouldn't be the default A joint report from the Australian Securities and Investments Commission (ASIC) and the Dutch Authority for the Financial Markets (AFM) https://download.asic.gov.au/media/5303322/rep632-published-14-october-2019.pdf

Recommendation 3.3 – provision of CDR to third parties

The serious issues that arise when a CDR Consumer provides CDR Data to a third party outside the CDR regime has been raised by Financial Rights in previous submissions.[2] Under the CDR consumers will have the ability to request their own data in a format that could be read by a computer program – whether it is in a pdf or other machine readable or screen scrapable format. It is this ability that enables non-CDR-accredited entities to potentially pressure individual consumers to provide the personal information outside of the CDR regime where there are few if any privacy protections in many circumstances – especially where the third part is not an APP entity..

While we support the provision of a warning to consumers when they are provided with their CDR Data – this will unfortunately not solve the problem. As acknowledged by the PIA and discussed above – disclosure is not likely to be sufficient to mitigate against the risks involved. Recent ASIC research found that:

> *There is emerging evidence from financial services regulators about the limitations of the effectiveness of warnings that firms have to display about the risks and features of certain products and services. … Warnings are not a cure-all for problems in financial services markets.*[3]

While helpful for some, desperate consumers, facing financial hardship will be motivated to ignore the warnings. Financially vulnerable consumers will sign up to any service if they are desperate enough, or perceive no real choice to solve their debt problems. Financial Rights knows from its work on the National Debt Helpline that many Australian consumers are vulnerable to the promises of debt management firms, quick-cash payday lenders, and online companies that promise to solve all of their financial problems for a fee or in exchange for their personal information.

Think about consumers applying for a financial check to obtain a rental property, struggling consumers who want to sign up with a debt consolidation service or pay day loan operator, or rural and regional Australians using the only store in town handing their details over.

The result is that the people who are most in need of protection – the financially vulnerable - will inevitably be provided the fewest protections under the CDR.

Warnings may very well prevent a large proportion of people from engaging in risky behaviour but it will be the vulnerable consumer, the consumer experiencing financial hardship that will be most at risk under the CDR regime as currently designed.

We believe further recommendations need to be made here.

---

[2] Including Financial Rights' submission to Treasury's initial Consumer Data Right, Privacy Impact Assessment, January 2019https://financialrights.org.au/wp-content/uploads/2019/02/190118_CDRPIA_Sub_FINAL.pdf

[3] Page 5, ASIC Rep 632: Disclosure: Why it shouldn't be the default A joint report from the Australian Securities and Investments Commission (ASIC) and the Dutch Authority for the Financial Markets (AFM) https://download.asic.gov.au/media/5303322/rep632-published-14-october-2019.pdf

The simplest solution would be to ensure that the *Privacy Act* and the APPs are modernised to extend the stronger CDR protections to all consumers no matter the situation. In this way consumers will be protected by the general law if their consumer data right data falls out of the CDR regime as is likely. We note that this is in essence being considered under the ACCC Digital Platforms Inquiry. We also note that Maddocks may not be in a position to make this recommendation given the scope and remit of this PIA.

Alternatively all handlers of CDR data from banks and credit unions (data holders), FinTechs and software developers (data participants) to accountants, financial advisors, mortgage brokers, insurance brokers, landlords or any other entity with even a remote interest in gaining access to sensitive, personal financial data should be accredited. This accreditation does not need to be onerous, can be appropriate to their use and be scalable.

Finally all screen-scraping and other unsafe data access, transfer and handling technologies should be banned as has occurred in the UK and elsewhere.

Recommendation 4 – CDR Consumer right to access CDR Data held by the Accredited Data Recipient

The PIA notes that the CDR regime does not afford similar rights to CDR Consumers as is provided for under APP 12 to request an Accredited Data Recipient to provide their CDR Data to them. This is a significant omission. The Explanatory Memorandum of the CDR Act states:

> *The primary aim of the CDR is to give consumers the ability to access and use more information about themselves, and about their use of goods and services, in a manner that allows them to make more informed decisions about both themselves and the good and services they use. By doing so, the CDR aims to increase competition, enable consumers to fairly harvest the value of their data, and enhance consumer welfare.*[4]

If it is empowering for consumers to be able to access their financial data from Data Holders – which is the entire raison d'être of the reform – then it is equally empowering for consumers to be able to access this information from Data Recipients. If this is not the case, then it provides an unequal playing ground between Data Holders and Data Recipients and increases risks for consumers to engage with open banking. Consumers must have the right to access this information and check the accuracy of the data held and confirm what data is being held.

Recommendation 5 - Draft Data Standards

We note that the PIA has identified that it is not easy to identify which of the Draft Data Standards are binding and which are not and which would assist CDR Consumers being informed. The PIA has subsequently recommended that the Draft Data Standards be recast into language that will allow CDR participants to easily distinguish which parts of the Draft Data Standards are binding legal requirements.

---

[4] Treasury Laws Amendment (Consumer Data Right) Bill 2019 Explanatory Memorandum https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6281_ems_58a7c56b-36e3-4388-acf8-58455b983a76/upload_pdf/698114.pdf;fileType=application%2Fpdf

We remain concerned that the CX guidelines are not binding upon Accredited Data Recipients and that therefore there are some standards that are binding and some that not.

The CX Guidelines are the practical expression of the standards and have some of the most direct impact upon consumers and the way they interact with their own financial data and the open banking system.

For example the CX Guidelines will provide guidance on how consent is managed and how consumers will control their data. If this design is inconsistent between each app or service then there will be serious confusion leading to poor outcomes. The guidelines need to be binding to avoid this confusion.

Another example is that the CX guidelines will also provide guidance on what consumers see first. The guidance can direct the industry towards prioritising what consumers need to see first – information that promotes a better understanding of their rights. However if left up to industry to decide, the industry is liable to prioritise what the industry wants the consumer to see first and conversely what they would want to de-prioritise and obfuscate. The information shown first could very well suit the industry's financial motivations rather than the consumers. This is important because consumers generally will not know themselves what is truly important to engage with when they manage their consents. The CX guidelines therefore need to require industry to assist consumers in an appropriate without industry interests misleading them. Without the guidelines being binding there is likely to be poor consumer outcomes.

This distinction between binding and non-binding inevitable will lead to regulatory arbitrage and provide significant scope to industry stakeholders to design interfaces that serve themselves well, and serve consumers poorly.

We therefore recommend that rather than merely distinguishing between binding and non binding requirements – that all the guidelines be binding and enforceable.

Recommendation 6 – Joint account holders in the banking sector

We strongly support Recommendation 6 that the Department further consider whether the CDR legislative framework implements an appropriate policy balance between the protection of the privacy of joint account holders, against the need to facilitate access to information by victims of family violence.

We recognise the tension between consumers gaining some benefit from the use of their data, and issues relating to privacy - and in the case of family violence, the individual's safety and ability to establish themselves financially after leaving a violent relationship.

Sharing of joint account data raises a number of issues - requiring special protections for all joint account holders, and also protections that apply when the bank is aware that there is, or may be, family violence. It is vital to ensure that:

- women experiencing family violence are not prevented from sharing their banking data due to requiring consent of the other party; and
- joint account holders are not unduly exposed by one party making decisions unilaterally about where joint personal information and data (banking transaction, payment and account data) goes.

We note that the PIA found that there is there is no ability for the Data Holder or Accredited Data Recipient to apply an exception to the general rules for joint account holders to *permit* the release of CDR Data for joint account holders.

We also note that there is little guidance on the level of evidence required for the Data Holder or Accredited Data Recipient to not update the joint account holder's consumer dashboard.

Perpetrators of family violence often try to sabotage the victim survivor's ability to establish a 'new life', for example by interfering with her employment, refusing to pay past household bills, or increasing legal costs unnecessarily. We are concerned that family violence perpetrators may refuse consent for a victim survivor to share joint data - and in many cases the victim survivor would not feel safe seeking consent.

While, in such cases, the bank should allow transfer of data without joint consent, it is important that the exemption from requiring joint consent doesn't benefit the perpetrator.

We also remain concerned about the inclusion of the physical address in the CDR data. Preferably, no personal contact information should be included in CDR data, although we recognise that this may be necessary for identification purposes in some cases but it is not clear whether this is necessary at all in a lot of the use cases.

In the end more guidance is required here.

Recommendation 7 – CDR Data which includes personal information about third parties

We agree with the PIA that there remains a significant issue regarding the risk to third parties arising out of the disclosure of CDR Data which includes information about transactions involving third party individuals. For example the inclusion of "Mums Birthday" in a transaction that has the potential to allow bad actors to gather identifying information.

We do not think that it is enough to merely publish information to support the current disclosure, including a description of the benefits for CDR Consumers and how this is balanced against the potential concerns third party individuals may have. This simply falls afoul of the failures of disclosure acknowledged by ASIC.

Requirements should be imposed upon Accredited Recipients (and Data Holders) to delete or de-identify after it is used or that this data be reconfigured to maintain the utility of such data but remove the risks.

Recommendation 8 – Seeking CDR Consumer agreement for an Accredited Data Recipient to become a Data Holder of CDR Data

We strongly support rules being introduced to ensure Accredited Data Recipients seek agreement from the consumer for them to become a Data Holder. The risk identified in the PIA goes directly to the issue of the complexity and inconsistency of consumer rights and protections at different stages and contexts of the data flow. This case demonstrated clearly that there are different protections in place for what essentially seems like the same thing to a consumer.

It remains confounding that the CDR has introduced such complexity and inconsistency when a standard consistent economy wide set of rights and protections would mitigate such issues.

Recommendation 9 – Adequate ACCC and OAIC resourcing

We support increased resourcing be provided to ACCC and OAIC.

Australians concern for the privacy with respect to their financial and other data should not be underestimated and Government must be prepared for an increase in complaints handling

Recommendation 10 – Consistent complaints processes

Financial Rights supports the recommendation to have a consistent complaints process. We have had the opportunity to read the submission by Legal Aid Queensland and support their response to this recommendation – particularly ensuring that complaints are cross referred appropriately and that consumers are referred appropriately to the relevant EDR scheme to deal with their complaint.

Concluding Remarks

Thank you again for the opportunity to comment. If you have any questions or concerns regarding this submission please do not hesitate to contact Financial Rights' Drew MacRae, Policy and Advocacy Officer on (02) 8204 1386.

Kind Regards,

Alexandra Kelly
Director of Casework
Financial Rights Legal Centre
Direct: (02) 8204 1370
E-mail: alexandra.kelly@financialrights.org.au

About Financial Rights

Financial Rights is a community legal centre that specialises in helping consumers understand and enforce their financial rights, especially low income and otherwise marginalised or vulnerable consumers. We provide free and independent financial counselling, legal advice and representation to individuals about a broad range of financial issues. Financial Rights operates the National Debt Helpline, which helps NSW consumers experiencing financial difficulties. We also operate the Insurance Law Service which provides advice nationally to consumers about insurance claims and debts to insurance companies, and the Mob Strong Debt Help services which assist Aboriginal and Torres Strait Islander Peoples with credit, debt and insurance matters.