Financial Rights
LEGAL CENTRE

Submission by the

Financial Rights Legal Centre

Australian Competition and Consumer Commission

CDR rules expansion amendments

Consultation Paper

October 2020

Financial Rights Legal Centre |PO BOX 538, Surry Hills 2010 | Tel (02) 9212 4216 |Fax (02) 9212 4711 |
info@financialrights.org.au | www.financialrights.org.au | @Fin_Rights_CLC | ABN: 40 506 635 273

About the Financial Rights Legal Centre

The Financial Rights Legal Centre 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. Financial Rights took over 22,000 calls for advice or assistance during the 2018/2019 financial year.

Introduction

Thank you for the opportunity to comment on the Australian Competition and Consumer Commission's Consumer Data Right consultation on proposed changes to the CDR Rules. This submission is made on behalf of the Financial Rights Legal Centre (**Financial Rights**).

The consultation proposes significant changes to the Consumer Data Right centred on introducing new tiered accreditation levels, a range of new consents and disclosures, a move to allow non-accredited parties to obtain highly sensitive consumer data without meeting safety and security standards and introducing new rules around the management of joint accounts.

Many of the proposed amendments disproportionately benefit of the FinTech sector and their commercial interests to the detriment of the needs and interests of consumers. Scant regard is given to the consequences to consumers in the proposals being put forward with the consumer interest largely distilled down to:

- increasing choice eg. "provide greater choices for consumers about who they share their data with"[1]; and
- improving experience and control: "adding flexibility and functionality to improve consumer experience in respect of the management of consumer consents…"[2]

Despite the consultation paper stating that the:

> *"ACCC has considered the following matters: likely effect of the Rules on: consumer, including the privacy or confidentiality of consumers' information."*

there are few if any new privacy protections being proposed and a significant number of derogations from the interests of consumers for a safe and secure data environment. The key consumer interest in a safe and secure data environment as well as an interest in a CDR that doesn't increase risk segmentation and price discrimination ultimately take a back seat to posited "increasing choice" and "improved experiences" interests.[3]

Arguments for increased choice and improved experiences sound consumer friendly on the surface and can be where they are accompanied with protections addressing other key consumer concerns, like security and privacy. However these latter protections are largely absent. This seems to be because, ultimately, increasing safety and security standards raise industry costs – an issue that trumps the consumer interest in a safe and secure data

[1] ACCC Consultation Paper, Page 4

[2] ACCC Consultation Paper, Page 4

[3] The consultation paper states that the *"ACCC has considered the following matters: likely effect of the Rules on: consumer, including the privacy or confidentiality of consumers' information."*

environment in almost every proposal. The proposals are – as asserted by the consultation paper – intended to reduce compliance costs for industry.

This is disappointing and it is left to the Maddocks Privacy Impact Assessment (**Maddocks PIA**) to at least identify the poor privacy outcomes of the proposals.

We remind the ACCC that there is strong evidence that consumers want a safe and secure data environment. The majority of Australians do not want companies sharing their information for secondary purposes. According to OAIC's 2020 Community Attitudes to Privacy survey the vast majority of Australians indicated they were uncomfortable with most types of information being shared with third parties:

> *Australians are increasingly questioning data practices where the purpose for collecting personal information is unclear, with 81% of Australians considering 'an organisation asking for information that doesn't seem relevant to the purpose of the transaction' as a misuse (up 7% since 2017)*[4]

The OAIC survey also found overwhelming consumer demand for stronger action from government with respect to privacy protections:

> *Eighty-three percent of Australians would like the government to do more to protect the privacy of their data.*[5]

On the flip side there is very little evidence supporting consumer interest in Open Banking and potential use cases. There has so far been minimal take-up in offers available since July 2020 and UK experience is such that there consumer uptake for Open Banking services is limited.[6] Whatever interest there is in expanding the CDR is purely supply driven – in the hope that a market can be created to support a fledgling sector.

Any moves to do so without strong privacy protections for consumers in place will inevitable undermine any potential success. We believe that these flawed proposals therefore set the FinTech sector and the CDR regime up for failure. This is because any potential for trust or confidence in the CDR regime will be damaged from the very start and be given a mortal blow with the first breach of data privacy.

Structure of the submission

It is our view that the Maddocks PIA presents a clearer structure to understand what is being proposed than the ACCC consultation paper since it draws out and delineates the true implications for consumers. This is because it places the consumer interest at the centre of its deliberations. We intend to base our submission on this clearer, more consumer focussed

[4] OAIC Australian Community Attitudes to Privacy Survey 2020, Page 7 https://www.oaic.gov.au/assets/engage-with-us/research/acaps-2020/Australian-Community-Attitudes-to-Privacy-Survey-2020.pdf

[5] OAIC Privacy Survey, Page 8

[6] https://www.finextra.com/newsarticle/35054/open-banking-year-two-insights-from-the-cma9

structure, both for ease and to ensure that the consumer interest is front and centre. We will therefore address our concerns with respect to the ACCC's proposals in five sections:

- Proposed changes to new levels and kinds of accreditation
- Proposed changes to consents
- Proposed changes to disclosure of CDR Data to Accredited Persons
- Proposed changed to disclosure of information relating to CDR Consumers to non-accredited persons
- Proposed changes to joint accounts

Summary of views

Tiered accreditation proposals

Financial Rights opposes the tiered accreditation proposal because:

- it relies on self-regulation to protect the consumer interest
- it introduces a complexity that by its nature will lead to consumer harm
- it fails to address safety and security risks created by differentiating tiers.

The ACCC must go back to the drawing board to design a tiered accreditation regime that:

- ensures that the consumer's best interest is the primary concern in designing a tiered accreditation process;
- does not rely on self-regulation;
- is simple for all participants including consumers to understand
- provides strong, consistent and unavoidable safety and security measures for consumers no matter which tier holds, collects, transfers, uses or analyses their data.

Consent proposals

Financial Rights opposes the proposals to change consent because:

- the range and complexity of consents will confuse consumers and undermine the concept of informed consent;
- the range and complexity of consents will lead to mistakes by industry;
- this new consent complexity is only due to the introduction of new forms of party disclosures including directing marketing and on-sale of data that provide little benefit and are more likely to lead to poor consumer outcomes;
- withdrawing the full range of consents would be harder;
- the proposed rules for amending consents will lead to undue pressure and subverts consumer control.

The ACCC must go back to the drawing board to design a consent model that:

- is simple for consumers (and industry) to understand and thus be genuinely informed;
- ensures that consumers can easily withdraw consent;
- prevents pressure or dark patterns to be used by CDR participants to maintain consents and ensures that consent is provide voluntarily
- provides consistency and transparency across the CDR environment through one centralised dashboard.

Disclosure of CDR Data to Accredited Persons proposal

Financial Rights opposes the proposed changes to the disclosure of CDR to accredited parties because:

- the distinction between Accredited Persons and Accredit Data Recipients is unclear and complex, which will lead to industry misunderstanding and likely breaches.
- this distinction becomes even more complex when combined with the complex consent proposals.
- proposal expands the ability for CDR parties to engage in inappropriate direct marketing.

Allowing the disclosure of information relating to CDR Consumers to non-accredited persons

Financial Rights opposes the ACCC's proposal to facilitate the disclosure of highly sensitive financial information relating to CDR Consumers to non-accredited persons without appropriate measures to protect the privacy, safety and security of consumers. This is because:

- Disclosure to a "trusted advisor" is not just inherently risky but is contrary to the entire point of the CDR to provide a safe a secure data environment
- Referring to "Trusted" advisors is misleading since many will not have to provide a safe and secure data environment
- Disclosure to "trusted advisors" facilitates the creation of two data protection regimes – one safe and secure environment, one with fewer if any consumer protections
- Voluntary consent is undermined
- Consumers will not understand the implications of consenting to disclosure of CDR Data, or a CDR Insight, to a recipient outside of the CDR
- There are no additional restrictions placed on what non-accredited parties can subsequently do with CDR data once obtained
- The proposed mitigants will not deal with the risks
- The high cost of accreditation should not outweigh the need for a safe and secure environment
- Consumer insights are more sensitive than raw data
- The consumer insights proposal places all the responsibility on the consumer

- Consumers will not have the automatic right to know what the insights are
- Consent from vulnerable consumers is unlikely to be free or fully informed
- Accredited persons do not have to comply with the CDR rules when transferring an insight.

The ACCC must go back to the drawing board and design develop a model for sharing of CDR data to new parties based on privacy-by-design and the following principles:

- consumers who choose to use and pass on their CDR data are afforded all the privacy and consumer protections under the CDR regime no matter who holds them;
- only accredited parties should be able to access and handle CDR data;
- all those who access and handle CDR must be required to meet high standards of security and safety as currently required under accreditation.

Any increased access to CDR data by interested parties that are not accredited should not even be considered until the Privacy Act has been reviewed (as recommended by the ACCC's Digital Platforms Inquiry) and increased consumer protections regarding the handling of data are increased as is the case in UK and Europe.

Joint account proposals

Financial Rights cannot support the current proposals for joint accounts because:

- in the absence of a physical or financial harm or abuse flag, there is a risk that one joint account holder will simply pressure the other to agree to the disclosure of joint account information;
- the requirement to share without the approval of the second joint account holder (in order to prevent physical or financial harm or abuse another joint account holder) assumes that there is a process or policy that enables a data holder to learn of such a threat – where there is no requirement to do so;
- the proposal only applies to Data Holders – Accredited Data Recipients and Accredited Persons are not required to give a joint account holder control over their data at this stage of the process
- there may be inconsistency between an online and an offline joint account management service
- there is the threat that joint account holders will not understand the consequences of selecting a disclosure option in the management service even with the information provided; and
- there is no clear and standardised level of evidence or guidance if an exception to the joint account system is to apply.

Further work is required to mitigate the risks including:

- requiring all CDR participants to provide easily accessible and obvious means for consumers to inform CDR participants of the threat of physical or financial harm or abuse,
- requiring all CDR participants to proactively identify such threats using analysis or other means.

Proposed changes to new levels and kinds of accreditation

Financial Rights has previously stated that we are not opposed to the development of new tiers of accreditation that take into account the different roles of different entities within the CDR system including intermediaries. This seems sensible. However we only do so if consumer data safety and security is prioritised. This proposal does not do this.

It is critical that no loopholes or exemptions are put in place for CDR data holders, recipients or intermediaries to take advantage of Australian consumers or undertake any form of regulatory arbitrage or avoidance. The tiered accreditation proposal put forward by this consultation paper fails this basic test. The reason it fails can be summarised as follows:

The tiered accreditation proposal relies on self-regulation

The consultation paper posits that:

> *"the aims of the accreditation process can be appropriately met through a tailored attestation and self-assessment process, complemented by a targeted audit and compliance program."*[7]

As we understand the proposal - sponsor accredited entities will be required to attest to the accreditor that its affiliate tiered partners meet the criteria set, and that there affiliates will be required to complete a self-assessment against Schedule 2 requirements and do so annually.

This proposed self-regulatory structure of accreditation will diminish trust in the CDR regime.

Self-regulation in the financial services sector (to which most accredited parties in Open Banking are entering) is a catastrophic failure that has led to the government about to introduce a co-regulatory scheme to introduce enforceable financial services codes of practice.[8] The lack of trust in the sector is rock bottom and while FinTechs are new players in the sector, community expectations are high that they must behave in ways that serve the consumer interest and expect all players in the financial services sector to meet high standards set by regulation. The time for self-regulation is over.

Critically the design of the proposal put forward does little to reassure consumers that their interests, safety and security will be prioritised.

There are few incentives on the sponsor to ensure compliance by affiliates since the sponsor will only need to take "*reasonable steps* to ensure its affiliates comply with the accreditation requirements and ongoing obligations of an accredited party."[9] There is no strict liability for any

[7] ACCC Consultation Paper, Page 10

[8] Treasury, Enforceability of financial services industry codes https://treasury.gov.au/consultation/c2020-48919f

[9] ACCC Consultation Paper, Page 15

breaches. "Reasonable steps" is so uncertain, loose and subjective as to be worthless in practice. As the Maddocks PIA points out:

> *For example, it is not clear whether a sponsor would satisfy the test by simply including an obligation in the CAP agreement which requires the affiliate to comply with the CC Act and the CDR Rules. If this would be sufficient, we suggest that it may provide little protection for a CDR Consumer if a restricted level Accredited Person does not meet its contractual requirements, noting that there is no obligation on a sponsor to enforce the CAP arrangement.*[10]

The only incentive to ensure entities meet the requirements is the post-facto threat of a potential targeted compliance and audit program – one presumably that will not subject all accredited entities all of the time. The self-regulation proposal therefore does little to prevent harm from occurring in the first place and inappropriately relies on identifying and addressing harm after it has occurred. This does little to protect consumers and will inevitably undermine trust in the CDR regime.

Arrangements between parties will be also fundamentally be commercial in nature and will focus on the commercial risks of the corporate entities and will not in their nature focus on the risks for consumers. This was the case in an equivalent scenario in general insurance where the only regulation of insurance investigations was the commercial arrangements between the insurer and their associated investigator entities. Insurers purported that these focused on ensuring that insurance investigations met high standards of conduct but led to a culture of egregious behaviour as outlined in Financial Rights' report *Guilty Until Proven Innocent*.[11]

Self-assessment also relies on commercial entities to self-identify breaches of the accreditation requirements. If self-assessment in existing financial services sector codes of practice is anything to go by then this is doomed to failure. For example the Life Insurance Code of Practice Code Compliance Committee has expressed serious concerns with insurers for self-reporting breaches of the Code – an obligation under their Code.[12] The same is the case with the Banking sector.[13] Given the huge compliance departments and resources of banks and insurers and their systemic failure to self-report breaches, we believe it is fanciful to think that smaller, under-resourced FinTechs and other entities will be able self-assess to an appropriately high standard.

---

[10] Maddocks PIA, Page 73

[11] Financial Rights Legal Centre, Guilty until proven innocent Insurance investigations in Australia, March 2016, https://financialrights.org.au/wp-content/uploads/2016/03/Guilty-until-proven-innocent.pdf

[12] "Despite the increase in self-reported breaches this year, information gleaned from investigating other allegations supports the Committee's continuing concerns that not all significant breaches are being reported." Page 3, Monitoring Compliance with the Life Insurance Code of Practice 2018-19 Retrospective https://www.afca.org.au/media/556/download

[13] "Overall, we believe there is still progress to be made to ensure all Code breaches are being identified and reported to us, and we encourage all Code-subscribing banks to make use of our guidance resources and reports to improve their Code compliance reporting." Page 8 BCCC Annual report 2019-20 https://bankingcode.org.au/app/uploads/2020/09/BCCC-2019-2020-Annual-Report.pdf

Furthermore it is the lack of ability to meet compliance costs of the accreditation regime that lies behind the reasoning being put forward to introduce a tiered accreditation in the first place. Introducing self-regulation here glosses over this reality and posits that these entities both at the same time cannot afford to meet accredited compliance costs but will somehow also be able to afford to introduce their own self-assessment compliance regime that meets the expectations of the accreditation process. This fundamental contradiction elides over the obvious point that entities will seek to save money on compliance and do the minimum they need to do, which will in turn not serve the interests, safety and security of consumers. A post-facto regime of potential targeted auditing will not serve as a strong enough incentive to prevent consumer harm – it has not done so in the self-regulatory environment of the financial services sector more broadly and there is nothing in this proposal to indicate it will be any different in the CDR.

We also note and agree with the risk identified by Maddocks that the CDR Rules do not deal with a situation where the relevant CAP agreement is terminated, or suspended, or expires.[14]

The tiered accreditation proposal introduces a complexity that by its nature will lead to consumer harm.

The Consultation Paper proposes to establish *four* additional levels of accreditation (and a further two categories for non-accredited parties to access CDR Data – to be discussed further later in this submission). These are:

- the unrestricted accredited parties
- data enclave accreditation,
- limited data accreditation and
- affiliate accreditation.

The complexity of varying requirements for each tier, with its complex array of requirements when tiers inevitably interact is such that:

- less experienced, sophisticated or resourced parties will take part in the scheme and not be able to meet their obligations and requirements;
- data is likely to be mishandled and not proactively managed;
- the large number of inconsistences, contradictions and incomplete provisions make it difficult for consumers, consumer representatives, industry, and regulators to understand the regime;
- consumers will prima facie not be able to be provide fully informed consent for the use, collection and disclosure of their data by these entities; and

[14]Maddocks PIA, Page 74

- consumers will not be able to identify or recognise when and where a breach of the accreditation rules has occurred and therefore not be able to assert their rights.

The complexity of the tiered accreditation proposal means that there are a number of gaps and inconsistencies – some of which have been identified but many others are inevitably going to either arise in the future or not be identified and lead to harms. For example:

- it is not clear under the proposal whether redundant data will be deleted by a provider under a CAP arrangement on direction by the principal;
- it is not clear whether there is a requirement for the provider to even comply with a direction.[15]
- It is not clear whether some accreditation levels will be required to keep records (rule 9.3(2)(i) only applies to principals)

To work, the proposed tiered accreditation system seems to be wholly dependent on commercial arrangements between the parties, which, again, will centre on dealing with the risks of the parties to the arrangement rather than focussing on the best interests of the consumer. It will also mean such rules and liabilities developed will be multiple, inconsistent and not guaranteed to deal with all the issues that will inevitably arise, leading to even further complexity, and a lack of transparency for consumers.

In addition there will be overlapping and inconsistencies between these arrangements and their legislative liabilities and obligations.

The tiered accreditation proposal fails to address safety and security risks created by differentiating tiers

Limited data accredited persons will be able to handle inherently sensitive financial data from consumers which will expose consumers to risks if mishandled. This is particularly the case once this data is combined and analysed with other data from other designated sectors.

The complexity of the system also raises the risk that some accreditation entities will deliberately or inadvertently collect data that does not fall within their permitted types. There are currently no protections in place to ensure that this does not occur outside of future commercial arrangements.

***

Given the fundamental problems with the proposal outlined above, we do not have confidence that the proposal will produce positive consumer outcomes and will in fact lead to consumer harm.

[15] See Maddocks PIA, Page 76

We note that the Maddocks PIA outlines some recommendations to mitigate the issues they have outlined – some of which we have repeated above. We however believe that the accumulation of issues outlined above and the inherently poor consumer outcomes that arise is disqualifying. We cannot support simply re-jigging the model to make improved on the fringes. We believe the ACCC must go back to the drawing board.

Recommendation

1. **Financial Rights opposes the tiered accreditation proposal as currently conceived. The ACCC must design a new tiered accreditation regime that:**
    a. **ensures that the consumer's best interest is the primary concern in designing a tiered accreditation process;**
    b. **does not rely on self-regulation;**
    c. **is simple for all participants including consumers to understand**
    d. **provides strong, consistent and unavoidable safety and security measures for consumers no matter which tier holds, collects, transfers, uses or analyses their data.**

Proposed changes to consents

Embedded amongst several proposals in the ACCC consultation paper is a significant change to the consent regime under the rules. Currently, consumers must consent to:

1. the collection of their data by an accredited party; and
2. the use of their data by an accredited party for specific purposes.

The details of these consents are limited to:

- the specific uses, and
- time information of the consent including when the consumer gave consent, for a single occasion or over a period of time and for what period and whether it is current.

The proposal being put forward will expand upon this concept and break it down further into separate and distinct forms of consent – 8 in total.

Firstly it is proposed that a new "disclosure consent" will be introduced into the rules. That is, an ADR will need to obtain the consent of the consumer to disclose the consumer's data to another party including:

a. another accredited person

b. to a so-called "trusted advisor"

c. anybody else seeking an insight

Secondly use consent will be broken down into separate types of uses including:

a. goods and services

b. CDR insights and

c. direct marketing.

The proposed CDR Rules categorise these into 8 form of consent[16]:

a. collection consents;

b. use consents relating to the goods or services requested by the CDR consumer;

c. use consents and disclosure consents relating to insights;

d. use consents and disclosure consents relating to direct marketing;

[16] Proposed Rule 1.10A(2)

e. use consents to de-identify some or all of the collected CDR data for the purpose of disclosing (including by selling) the de-identified data;

f. use consents relating to general research;

g. Accredited Person disclosure consents;

h. Trusted Advisor disclosure consents

At first glance it may seem to be a good idea to separate out and unbundle these consents. Surely this will give consumers more control? And yes, if consumers were rational, informed and engaged with providing their express, specific, and time limited consent, with the ability to understand, amend and withdraw their consent in a clear and simply manner, then yes this would be a positive step.

However in the real world, consumer behaviour is not rational, they are likely to be far from fully informed when the concepts involved are so complex, consumers rarely are free of undue influence and in many situations will be completely disengaged with the process – ticking yes to boxes like a user signing up to the proverbial iTunes agreement.

The complicated new consent regime has a multitude of serious problems that will lead to poor consumer outcomes, the sum total of which means that Financial Rights cannot support the proposal. We outline the problems are as follows.

The range and complexity of consents will confuse consumers and undermine the concept of informed consent

If the proposal were to move forward it is highly likely that consumers will have no idea what they are consenting to. The only thing that the proposal seeks to do to mitigate the inevitable issues with comprehension and understanding is that the new rules provide:

- a statement of the fact of a propose use or disclosure and
- a link to the provider's CDR policy and
- a statement that the consumer can obtain further information [17]

In no way do any of the above lead to a scenario where the consumer will be informed. It requires the consumer to take additional steps to seek clarity and information – a step that we already know from the prevalence of iTunes-like agreements that they will not take. Also it is a step that clearly contravenes Rule 4.10(b). It also places the entire responsibility on the consumer to read the CDR policy, understand the policy and its potential consequences and make a decision based on that full understanding of the consequences of that policy. That is unreasonable, unlikely to ever happen and counter to all that we have learnt about the behaviour of consumers online.

[17] See Rule 4.11.

The concept that consent must be informed necessarily requires the avoidance of relying on long form agreements or policies.[18] Genuinely informed consent in an online environment requires a fundamental re-think of the consent process. What is being proposed here however is essentially business as usual – where consumers click and tick what they need to get the service without understanding what they are agreeing to. The new consent proposal taken as a whole fundamental undermines the concept of informed consent – as required under Rule 4.9(c).

It is well understood by industry, government and regulators that disclosure as a tool has failed. This proposal perpetuates these failures to the detriment of potential users of the CDR regime.

The range and complexity of consents will lead to mistakes by industry

While the proposal is so complicated that it will be near impossible for a lay person to understand and track in the real world it is also confounding for those with a close interest in the detail of the regime. The regime was already complex enough without these added layers of confusion.

The complexity of the consent regime will make it extremely difficult for industry participants to understand the regime and their obligations at each and every step of the new information flows. This is likely to lead to consumer data being mishandled, not being protected appropriately, or actively managed that serves the consumer's interest. The more breaches and mistakes, the more the regulatory bodies will need to supervise and retrospectively regulate, and the more likely consumers will lose trust in the regime and either avoid taking part or withdraw from the regime altogether.

We do not believe that a clearer guidance will suffice. The complexity is such that a clearer guidance is impossible.

The new consent complexity is only due to the introduction of new forms of party disclosures including directing marketing and on-sale of data that provide little benefit and are more likely to lead to poor consumer outcomes

The introduction of a complex and confusing consent regime including "disclosure consents" is only necessary because of the introduction of series of pro-industry measures that will lead to poor consumer outcomes. These new measures are seeking to allow:

- the sale of data;
- an expansion of direct marketing beyond the initial purpose of the primary service;
- the use of data for so-called "research" purposes

[18] The proposal also repeats a problem that exists in insurance where insurers are required to disclose to an insured how a policy veers from standard cover and can do so by simply providing a Product Disclosure Statement..

- the release of CDR data to certain non-accredited professions into unsafe and insecure data environments with little to no consumer protections; and
- the release of CDR data in the form of "insights" to anyone at all increasing risks to the consumer.

None of these five new forms of disclosure actually benefit consumers in any real sense. Each one merely leads to increased chances for exploitation and other poor outcomes. Financial Rights has long argued for the need to curtail such forms of disclosure to create a safe and secure environment for consumers. Their introduction undermines this:

The sale of data

Currently an ADR is prevented from selling the data it receives unless the CDR data is de-identified in accordance with the CDR data de-identification process: Rule 1.17, 4.12.

The proposed amendments removes the restriction on an Accredited Person asking for consent to sell CDR Data, as well as derived insights and commercial research by data recipients.

What is even more disturbing is that there are no requirements in the proposal for the consumer to be informed or choose whether they can consent to the sale of their CDR data, An accredited person only has to seek consent that falls within a category of consents: proposed Rule 4.12(3). In other words consent to sell data can be bundled – a concept that was meant to be eradicated by another important element of consent – that consent be "specific as to purpose." The proposal of categories of consent therefore fundamentally undermines this arm of consent at Rule 4.9.

To be clear – there is little to no benefit for a consumer to have their data sold (de-identified or otherwise). The only benefit usually asserted by industry is that the sale will provide them with income that will lead to cheaper prices for the goods or services that they provide to the consumer but it is unclear whether this is ever the case.

On the flip side there are many problems to the sale of data. Selling data can lead to unscrupulous or disreputable international or Australian parties to misuse data through spamming, hacking or other activities that don't comply with the law or meet community expectations. Even the sale of de-identified data can lead to serious problems in profiling consumers and voters in ways that lead to poor societal outcomes. There is also the risk that some de-identified data can be used to re-identify consumers when combined with other sets of data – leading to even greater risks.

Direct marketing

The current rules limit direct marketing to "information about the benefits of existing goods or services" [Rule 7.5(3)]. This ensures that Open Banking apps that promote goods that are being sought by the consumer in their app (such as service that seeks better deals for a credit card) are able to do so.

The proposal to permit accredited persons to collect and disclose CDR data between themselves in order to offer goods and services to consumers is a vast expansion of the current concept of "direct marketing" under the rules.

Such an expansion provides the very real potential to increase predatory targeted marketing practices, particularly with respect to financially vulnerable people. We provide further details on our concerns below under the section "Proposed changes to disclosure of CDR Data to Accredited Persons".

Research

Current rules limit ADRs from using CDR data for purposes beyond what is reasonably needed in order to provide the requested goods or services. This precludes consumers from consenting to ADRs using their CDR data for research purposes where it does not relate to the goods or services requested.

The consultation proposes to remove this restriction. We hold serious concerns with respect to this proposed change.

Firstly the concept of research is not confined to non-commercial, academic research or any other socially beneficial form of research in the public good but is broad enough to include product development, business development, market research and anything up to and including the building of data profiles unrelated to their provision of a specific service to the consumer. This is concerning and runs counter to the original principles of CDR to confine the use of data to the specific use cases for good or services provided.

The proposed amendments require that when an accredited person is asking a CDR consumer to give consent for this purpose, they must provide a link to the description in the Accredited Data Recipient's CDR Policy which specifies the research to be conducted, and any additional benefit to the CDR Consumer for consenting to the use of their CDR Data. However, this contravenes Rule 4.10(b)(i) which states that:

> *An accredited person's processes for asking a CDR consumer to give and amend a consent … must not … include or refer to other documents so as to reduce comprehensibility*

Furthermore the proposed rules around research consent undermines the voluntary nature of consent. The proposal ensures that the consumer needs to be informed of any additional benefit to be provided to the CDR consumer for consenting to the use[19] and the consultation paper foresees that:

> *The benefit to the consumer could be, for example, the ADR paying a fee to the CDR consumer or providing a discount on services provided to the CDR consumer. If the consumer consents to*

[19] Proposed rule 4.11(3)

this research use, this would allow the ADR to use the data collected for providing a good or service for other activities such as product development or business development.[20]

In attending a CDR standards workshop one, FinTech representative asserted that CDR Data Recipients should be able to offer consumers something in return for consenting to the holding or de-identification of data - that is they plan to have their client FinTechs offer "buckets of chicken", movie tickets, vouchers, cash or other financial incentives to consent to the collection and retention of de-identified data. There is nothing in the proposed rules that would stop the above from occurring and would be open to abuse.

This is deeply concerning and fundamentally undermines the concept of consent as detailed under the rules ie voluntary, express, informed, specific as to purpose. Will people really be freely consenting to a particular use if that consent is based on an incentive unrelated to the use? Without the direct link the additional benefit acts as a bribe to induce consent for a purpose that the consumer would not be otherwise interested in. Consumers will not be fully informed of the consequences and risks of what they are signing themselves up to and will be distracted by offers of free movie tickets.

Trusted advisors

Disclosing CDR data to non-accredited parties is currently not allowed under the current rules for very good safety, security and privacy reasons. The consultation paper proposes to remove this restriction and allow the disclosure of highly sensitive CDR data to be disclosed to non-accredited persons with no safety and security protections in place.

The proposal undermines the entire raison detre of the Consumer Data Right and its safeguarded environment by facilitating the movement of highly sensitive financial data and other consumer data to unsafe and insecure environments with little to no protections or redress for the consumers when things will inevitably go wrong.

Any benefits that consumers may receive from the passing of their data to the professions proposed is offset by the lack of security standards applied to these entities and the fact that the strong consumer protections afforded by the CDR regime do not move with the data – leaving consumers vulnerable to lower privacy standards under the current woefully inadequate and out of date privacy regime.

For further information on this critical issue, please see the section titled "Proposed changed to disclosure of information relating to CDR Consumers to non-accredited persons" below.

Insights

As with the above disclosing CDR data to non-accredited parties is currently not allowed under the current rules for very good safety, security and privacy reasons. The consultation paper proposes to allow consumer to provide to "any person" their CDR data by a consumer in a so-called "CDR insight" form.

[20] ACCC Consultation Paper, Page 48

As with the trusted advisor issue above, any benefits that consumers may receive from the passing of their data to the professions proposed is offset by the lack of security standards applied to these entities and the fact that the strong consumer protections afforded by the CDR regime do not move with the data.

The proposal is deeply flawed for reasons that we explain in the section titled "Proposed changed to disclosure of information relating to CDR Consumers to non-accredited persons" below.

Withdrawing the full range of consents would be harder

Given the multiplicity of consents, and different timings relating to the different requests and complexities involved in the amending process, withdrawing the full range of consents has been made more difficult. The complexity and range of consents will lead to many not understanding that they may have only withdrawn or amended one form of consent without withdrawing all their consents, being alerted to their other consents remaining live or not being alerted to the right to have their data deleted. The proposal, for example:

- does not alert a consumer who is amending their consent to the fact that they may wish to withdraw all their use, collection and disclosure consents.
- does not alert a consumer that their disclosure consents to an ADR do not expire (and can continue to be disclosed and sold) when the ADR becomes a Data Holder as defined under the complex regime; and
- merely provides the consumer the ability to elect to delete redundant data rather than erring on the side of automatically or pre-filling a box to delete the data.

CDR participants must be required to give consumers the opportunity to withdraw all their consents in one step. CDR participants must then be required to give consumers the opportunity to delete their data to the full extent that they can in the next step. Otherwise withdrawing of consent will never be easy and the complexity will be used and misused to maintain a consumer's custom without their full knowledge or awareness.

The proposed rules for amending consents will lead to undue pressure and subverts consumer control

The proposed new ability to amend consents (rather than removing an existing consent and replacing it) expands the range and complexity of choices for consumers in line with the expansion and complexity of the range of consents. It is proposed that consumers will be able to to:

- add or remove uses
- add or remove data types
- add or remove accounts
- amending durations
- add or remove data holders.

While on the surface this looks like a positive – the consultation paper asserts that this will allow "consumers to have more control over their consents" – the increased complexity will mean that it is less likely that consumers will understand what they are actually consenting to.

The proposal also adds to the complexity by allowing

> *"accredited persons.. to determine the best approach for their particular good or service. For example, some accredited persons may offer the ability to amend multiple attributes in one consent process, while others may not."*[21]

This ensures that the consumer experience will not be consistent across the CDR environment.

This is exacerbated by merely giving ADRs *the option* to present a consumer's consent as pre-selected options where the consumer has previously selected a particular option in the past. This means that some ADRs can provide a screen where all the consents are left blank and a consumer would have to tick all the boxes – potentially inadvertently overriding previously chosen consents. This is far from ideal from the perspective of ensuring that consumers are informed when they are making a consent[22].

The consultation paper claims that the separate consents approach and the potential for pre-selected options to be made available actually streamlines the process allowing the consumer to focus on the changing attribute.[23] The problem is that by focusing on changing the attribute the consumer may not focus on the other consents that they should be considering.

The proposal also introduces the ability for an accredited person to invite a consumer to amend their consent to better enable the provision of goods or services but that this invitation must not:

- give the invitation any earlier than a *reasonable period* before the current consent is expected and
- give more than a *reasonable number* of such invitations within this period.

The concept of reasonableness is subjective here and will only be settled after complaints or harms occur. It is more appropriate to set maximum amounts here.

Outside of an invitation to amend – there is nothing in the rules to ensure that a consumer would know that they can amend their consents under the proposed rules. This works against the concept of consumers having control over their own data if that ongoing control is not made clear to the consumer.

The consultation paper also proposed that accredited persons "should be required to offer consumers the ability to amend the consent in the consumer dashboard to the extent possible"[24] but that "For some use cases that may mean only offering consumers the ability to amend a consent to associate a new account or a new data holder with the arrangement." This means that

---

[21] ACCC Consultation Paper Page 42

[22] Proposed Rule 4.12C

[23] ACCC Consultation Paper Page 42

[24] ACCC Consultation Paper Page 42

– as elucidated in the example on page 43 – some use cases will not be able provide the ability to amend some consents. We disagree with this approach. If all possible consents were made available to the consumer to amend – if they were to seek to amend a consent that undermines the ability to use the service, they should be alerted as such and be given the option to withdraw their consent to the service and delete their data. Otherwise consumers will not be fully informed and not have full control over their consents.

Other issues with the consent proposals

Financial Rights also agrees with the other risks identified in the PIA. These include:

- ***There is a lack of timing requirements for when consumers should be told certain things at certain points in the information flows*** – all of which should be instantaneous given the technology.
- ***Amendments to Data Holder authorisations will not be presented on Data Holder Consumer Dashboards*** – which is inconsistent and confusing.
- ***Proposals regarding disclosure consents between accredited persons and accredited data recipients includes a number of gaps, inconsistencies and complexities that do not serve consumer interests*** – this is discussed in more detail in the following section.

Given the above problems, we do not have confidence that the proposal regarding consent will produce positive consumer outcomes and will in fact lead to consumer harm.

As with the tiered accreditation proposal we note that the Maddocks PIA outlines some recommendations to mitigate the issues they have outlined. We however believe that the accumulation of issues outlined above means that the ACCC needs to go back to the drawing board.

Recommendation

3. **Financial Rights opposes the proposals to change consent as currently conceived. The ACCC must design a consent model that:**
    a. **is simple for consumers (and industry) to understand and thus be genuinely informed;**
    b. **ensures that consumers can easily withdraw consent;**
    c. **prevents pressure or dark patterns to be used by CDR participants to maintain consents and ensures that consent is provide voluntarily**
    d. **provides consistency and transparency across the CDR environment through one centralised dashboard.**

Proposed changes to disclosure of CDR Data to Accredited Persons

The proposal to introduce changes to the disclosure of CDR data to accredited persons within a new complex ecosystem of Accredited Data Recipients under the tiered accreditation model is seriously flawed and requires rethinking. We outline our concerns below:

The AP/ADR distinction is unclear and complex, which will lead to industry misunderstanding and likely breaches.

Under the CDR rules there is a distinction between an Accredited Person and an Accredited Data Recipient. Formally the distinction is that a:

- person is an Accredited Person if they hold an accreditation under section 56CA(1) of the CC Act;
- a person is an Accredited Data Recipient of CDR Data (under section 56AK of the CC Act) if:
    - they are an Accredited Person;
    - the CDR Data is held by (or on behalf of) the person;
    - the CDR Data was disclosed to the person under the CDR Rules; and
    - the person is not a Data Holder for the CDR Data.

In practice this means that a person who has received accreditation under the CDR Act, but has not yet received any CDR Data from another Data Holder, will be an "accredited person" but not an "accredited data recipient."

The distinction is important in the context of the new proposal for Combined Accredited Person (CAP) arrangements under the tiered accreditation proposal – which purports to

> "*provide to range of options for accredited parties to work together and to support the development of a varied and innovative service offerings to consumers*"[25]

CAP arrangements are arrangements between accredited parties to essentially permit an accredited outsourced service provider to collect CDR data on a person's behalf. The new proposals are about enabling a restricted accredited person to work with an unrestricted accredited person:

- to support data enclave restricted accreditation (where it would be mandatory to use a CAP arrangement), or

[25] ACCC Consultation Paper Page 24

- to support affiliate restricted accreditation (where it would be optional to use a CAP arrangement)

under the new complexities proposed in tiered accreditation. The key problem – as pointed out by the Maddocks PIA – is that it is:

> *difficult to determine from the proposed amendments which entity or entities will be considered to have 'collected' CDR data in the context of a CAP arrangement, and when that entity or those entities will be considered to be 'holding' CDR data*
>
> …
>
> *This clarity is important because it affects whether the provider is considered to be an 'accredited person' or an 'accredited data recipient' at various stages, which then affects other legislative obligations (including the application of the privacy safeguards).*[26]

In short, the original complicated flow of information, and rights and obligations applying at different stages of the process has been made exponentially more complicated to the point that the consultation paper doesn't attempt to even lay this out in a manner that is clear, transparent and comprehensible. The gaps and consequences that are created are essentially left to the industry to figure out. This will lead to inevitable mistakes – mistakes that are likely to be in favour of the commercial interests of industry not the interests of the consumer.

Furthermore it is unclear from the proposal whether ADRs will be required to check credentials of an Accredited Person. This could lead to disclosures of CDR data to unaccredited persons, since accreditations may have lapsed, revoked or suspended.

The AP/ADR distinction combined with the complex consent proposals adds even further complexity and gaps.

The distinctions and varying obligations of APs and ADRs also means that:

- ***It is not clear under the proposal when one consent expires (such as a collection consent held by Accredited Person) what happens to the other consents in the process (such as ADR's disclosure consent.***

  Rule 4.14(1A) states that this will occur when the accredited person receives the notification but then also states that if one of those consents expires, the other expires at the same time. This adds complexity and a lack of clarity to a process that already relies on the fact that a data holder only needs to give effect to a withdrawal of authorisation "as soon as practicable and in any case within 2 business days after receiving the communication." This remains a strange case of friction in a process that is frictionless in most if not all other cases.

- ***consumers will be kept in the dark about certain consents.***

  As pointed out by the Maddocks PIA:

[26] Maddocks PIA page 46.

Under the proposed amendments to the CDR Rules, an Accredited Data Recipient (A1) is not obliged to seek an AP Disclosure Consent from a CDR Consumer, even if the CDR Consumer has provided a Collection Consent to the relevant Accredited Person (A2).

In addition, even if the CDR Consumer has provided an AP Disclosure Consent to the Accredited Data Recipient (A1), that Accredited Data Recipient (A1) is not obliged to provide the CDR Data to the nominated Accredited Person (A2). Accordingly, there is a risk that a CDR Consumer will not receive an appropriate level of control or oversight over the status of their Accredited Data Recipient Request, or their CDR Data[27]

- ***amendments to AP collection consents may not carry over to ADR disclosure consents.***

  This is because there are no requirements to either amend the disclosure consent or invite the consumer to amend the disclosure consent.

- ***ADRs may not be aware of a consumer withdrawing their collection consent provided to an AP***

  This is because they are only required to notify if the consent expires (as opposed to withdrawal).

The proposal expands the ability for CDR parties to engage in inappropriate direct marketing

The proposal to permit accredited persons to collect and disclose CDR data between themselves in order to offer goods and services to consumers is essentially a vast expansion of the current concept of "direct marketing" under the rules.

The current rules limit direct marketing to "information about the benefits of existing goods or services" [Rule 7.5(3)]. This ensures that Open Banking apps that promote goods that are being sought by the consumer in their app (such as service that seeks better deals for a credit card) are able to do so The ACCC's original position was that:

> *In relation to on-selling of data and use of CDR data for direct marketing, the ACCC's current position is that it proposes to make rules that will prohibit the use of CDR data for these purposes.*[28]

The reason for limiting on-selling and direct marketing is clear. The CDR regime provides the very real potential to increase predatory targeted marketing practices, particularly with respect to financially vulnerable people. Consumers struggling with debt are often the most profitable customers for banks and lenders and are constantly barraged with marketing offers for financial services products.

The new proposal however now opens up the CDR to these very practices.

---

[27] Maddocks PIA Page 61

[28] ACCC Consumer Data Right Rules Framework September 2018 https://consultation.accc.gov.au/communications-1/consumer-data-right-rules-framework-consultation/supporting_documents/ACCCConsumerDataRightRulesFramework.pdf

The proposal will allow an ADR (with the consumers consent) to transfer the consumer's CDR to another ADR if and send them

> *(iv) information about other goods or services provided by another accredited person, if the accredited data recipient:*
>
> > *(A)* ***reasonably believes that the CDR consumer might benefit*** *from those other goods or services; and*
> >
> > *(B) sends such information to the CDR consumer on* ***no more than a reasonable number of occasions****;*

The construction of "*reasonably believes that the CDR consumer might benefit from those other goods or services*" is subjective, completely open to abuse and ultimately is no restriction at all. Every ADR could easily assert that they reasonably believe that a CDR consumer might benefit from any and every other good or service they may be offered.

In the financial hardship space – for example - an ADR providing credit switching services could easily argue that every other financial service provided by every other ADR could be good for any and every consumer. This is because:

(a) it is defensible to assert that it was reasonable because the service purports to help people when that may not be the case in reality;

(b) they have a commercial (conflict of) interest in selling this data that would necessarily outweigh the consumer's interest**.**

It is hard to conceive of a situation where there wouldn't be at least some plausible argument to be put forward by an ADR. It is clear that once a consumer experiencing financial hardship is identified by an ADR they will be direct marketed to by debt management vultures and other services. This is only exacerbated by the proposal for self-regulation in tiered accreditation levels.

Placing the decision in the hands of the conflicted ADR ultimately undermines a consumer's ability to control the use of their data despite potentially consenting to the disclosure in the first place. It is clear that a CDR consumer will be asked to consent to very broad disclosure uses that will not specify the potential consequences of the disclosure and the current and future arrangements in place. It hands over too much control to the accredited person and is likely to harm vulnerable consumers.

The further construction of sending information *"to the CDR consumer on no more than a reasonable number of occasions"* is also ludicrous. One person's reasonable is another's spam. Given accredited parties will be left to self-regulate, an ADRs view of a reasonable number will be very different to community expectations.

Target marketing of products to particular groups of consumers is not new. In consumer lending, technology can be used to identify consumers who are likely to be profitable, tailor and price products that the most profitable customers are likely to accept, and develop strategies to reduce the likelihood that the most profitable customers will close their accounts.

Consumers struggling with debt are often the most profitable customers for banks and lenders and are constantly barraged with marketing offers for financial services products. It is often

argued that it is not in the interests of lenders to extend credit to people who are unable to repay. However, our experience suggests that many consumers struggle for years at a time to make repayments to their credit accounts without ever reaching the point of default, but paying significant amounts of interest. These customers are very profitable for lenders, despite the fact that repayments are causing financial hardship.

Seemingly 'free' or 'freemium' business models could also see an increase in direct marketing, on-sale of transactional data, or the commission-based selling of unsuitable financial products, because it is a way for firms to monetise what they do without requesting a fee upfront.

It is clear that many business models will based in part or in whole on selling data for direct marketing purposes. It is disappointing that pressure from the FinTech sector on to allow this has been accepted by Government and in this current proposal.

It is clear that the proposal is only in the interest of industry and is not in the interests of consumers. The only argument that this could be in the interests of consumers is that consumer might benefit from a new good or service. Selling consumers more goods and services may serve industry well and may serve some consumers well, but is rarely in the best interests of consumers experiencing financial hardship.

We stand by our long held view that direct marketing that arises as a secondary purpose should be prohibited outright.

Recommendation

4. **Financial Rights opposes the proposed changes to the disclosure of CDR to accredited parties.**

Proposed changed to disclosure of information relating to CDR Consumers to non-accredited persons

The most egregious proposal in the consultation paper involves the proposal to allow the disclosure of highly sensitive CDR data to be disclosed to non-accredited persons with no safety and security protections in place.

While Financial Rights acknowledges that the utility of the CDR will require involvement of more parties including accountants, financial advisors etc, the model being put forward places the interests of these parties well ahead of the interests of consumers to share their data in a safe and secure data environment.

The proposal undermines the entire raison detre of the Consumer Data Right and its safeguarded environment by facilitating the movement of highly sensitive financial data and other consumer data to unsafe and insecure environments with little to no protections or redress for the consumers when things will inevitably go wrong.

We reiterate once again that the Open Banking Review Final Report recommended that the CDR legislation should be a closed system to prevent any CDR data being provided to any non-accredited entity.

> ***Recommendation 2.7 accreditation***
>
> *Only accredited parties should be able to receive Open Banking data. The ACCC should determine the criteria for, and method of, accreditation.*[29]

The reasons for a closed system were detailed as follows:

> *Accreditation would create a list of parties who are considered trustworthy, due to their compliance with a set of requirements. A customer's banking data is valuable information and its misuse can lead to damage or financial loss. Those who receive and hold data under Open Banking should therefore be required to safeguard that information.*
>
> …
>
> *From the customer's perspective, an accreditation process is desirable. Accreditation would allow customers to determine with greater ease which data recipients meet the Standards and may, as a result, be considered trustworthy. An accreditation process should inspire confidence amongst customers to share their data with recipients that the customer has chosen to trust. An accreditation process would also provide some level of customer protection from malicious third parties.* [30]

[29] Page 23, Open Banking: customers, choice, convenience, confidence, December 2017 https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking-_For-web-1.pdf

[30] Page 23, Open Banking: customers, choice, convenience, confidence, December 2017

The Report also noted that there is a closed system within the only other major developed country with Open Banking.

> *The UK has decided to limit access only to accredited third parties known as 'whitelisted parties'. A bank would only comply with a customer's request to transfer their data to a third party if that party is 'whitelisted'. This limitation of access reduces risk and gives users greater confidence in sharing data. The EU's PSD2 also contains an accreditation process.*[31]

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.

The fact that the ACCC proposal does not include such accreditation is counter to the consumer interest and counter to all CDR stakeholders including the FinTech sector who have an interest in promoting a safe and secure data environment.

Financial Rights will now explain in more detail we oppose the two distinct proposals being put forward.

Disclosure to a "trusted advisor"

Disclosure to a "trusted advisor" is not just inherently risky but is contrary to the entire point of the CDR to provide a safe a secure data environment

Disclosure to a "trusted advisor" (**TA**) is –inherently risky. It also undermines the stated intention of the CDR – that is, to develop a ***safe and secure*** environment in which consumers will be able to use and share their data. These facts are acknowledged by the consultation paper.

> *However, we recognise that allowing the disclosure of CDR data to non-accredited persons is a significant shift in the CDR regime, which currently only permits accredited persons to receive CDR data (with the exception of outsourced service providers). While non-accredited parties are often subject to regulatory requirements, including under professional regulatory regimes and protections set out in the Privacy Act 1988, they would not be subject to the requirements of the CDR framework. As such, there would be no obligation on non-accredited parties to delete data in accordance with any election made by the consumer as this election only applies to CDR data held by an accredited person.* [32]

But rather than recognising that this should disqualify any access by non-accredited parties - as it would fundamentally undermine the point of the CDR regime – the consultation paper states that this should merely limit the leakage of such data:

> *We therefore consider that these kinds of disclosures should be limited.*[33]

---

[31] Page 23, Open Banking: customers, choice, convenience, confidence, December 2017

[32] ACCC Consultation Paper, Page 29

[33] ACCC Consultation Paper, Page 29

The limits that are proposed are:

- The scope of non-accredited access will be limited to a list of so-called "trusted advisors"
- The consumer will need to consent to the disclosure
- Records will need to be kept of the disclosure
- The ADR may need to comply with standards set by the Data Standards Chair including providing a warning that the non-accredited person may not be subject to the *Privacy Act*.
- Allowing access to a consumer's CDR data "to any person" outside of the "trusted advisors" category, limited to mere "CDR insights".

Each of these so called "limits" are no limits at all and will not protect consumers from the consequences of inevitable data breaches, and poor behaviour that will almost certainly take place by bad actors. These are discussed below.

Referring to "Trusted" advisors is misleading since many will not have to provide a safe and secure data environment

The ACCC proposes that "trusted" advisors be allowed to access consumer's sensitive data. Using the word "trust" is misleading. The moniker both:

- assumes that the consumer trusts their advisor without acknowledging that they may not be in fact worthy of trust particularly given there is no obligation on many of the professions to keep their data safe and secure; and
- creates a false impression that such professions should be trusted to handle their sensitive data safely and securely while again not imposing any requirements on those advisors to do so.

In fact the proposal acknowledges that many advisors will not have to meet even the basic requirements under the current Australian Privacy Principles. As we have made clear a number of times to the ACCC and to the Treasury - the introduction of the CDR regime has created multiple levels of privacy standards for different people that will apply at different times to consumers seeking protection, security and redress when something goes wrong. They include:

- CDR Privacy Safeguards– essentially strengthened versions of the Australian Privacy Principles (**APPs**);
- the *Privacy Act* safeguards as detailed under the APPs; and
- general consumer protections and law applying to those holders of consumer data that are *not* "APP entities" as defined under the APPs, ie all private sector and not-for-profit organisations with an annual turnover of less than $3 million.

If non-accredited parties are ultimately able to access CDR data, this will lead to the following two situations that provide lower standards of consumer protection:

1. CDR data accessed and held by non-accredited parties who are "APP entities"[34] will be subject to the APPs, not the CDR privacy safeguards.
2. CDR data accessed and held by non-accredited parties who are not "APP entities" will neither be subject to the APPs nor the CDR privacy safeguards but only general consumer protections and law.

Allowing non-accredited entities the ability to access CDR against the recommendation of the Open Banking Report creates a significant leakage point for CDR data to fall outside of the system, whereby consumers will be provided fewer or lower standard protections or in some cases, no realistic privacy protections at all if or when a breach or problem arises out of the use or misuse of this CDR data.

No part of the proposal mitigates this huge risk.

It has been argued that the handling of consumer's financial CDR data by advisors will be not any different to what currently takes place. The consultation paper states:

> *Consumers routinely share their banking data with members of these professionals and we consider there will be consumer benefit in allowing this to occur via the CDR.*[35]

This is a false equivalence. The CDR data that would be able to be accessed would be of such a volume (and accessed and analysed at a greater speed) that by its very nature this interaction will increase the risks to the consumer if any material were to be breached by the advisor due to poor security processes.

But even if it were accepted that the handling of a consumer's financial CDR data by advisors is not any different to what currently takes place – this fundamentally undermines the point of the CDR – that is: the CDR is meant to increase the safety and security of the sharing one's data. This proposal essentially acknowledges that that will not occur and sets up dual consumer data protection systems.

The classes of professions that are currently proposed to be included as "trusted advisors" include: accountants, lawyers, tax agents, BAS agents, financial advisors, financial counsellors, and mortgage brokers.

Given the multiple inquiries and the recent royal commission into financial services the reputation of financial advisors and mortgage brokers is such that "trusted" advisor is particularly in-apt.

[34] Australian and Norfolk Island Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses

[35] ACCC Consultation Paper Page 30

Disclosure to "trusted advisors" facilitates the creation of two data protection regimes – one safe and secure environment, one with fewer if any consumer protections

The proposal to allow CDR data to be transferred to non-accredited parties facilitates the creation of two data protection regimes by providing an incentive for parties to not become CDR accredited and consequently not ensure a safe and secure data environment.

The proposal essentially says that some entities who really should be accredited (with the safety and security requirements met) do not have to be accredited. Why then would these parties ever decide to take part in the CDR regime when they don't have to? Why would they want to team up with a FInTech to produce a safe data service? There very well may be parties who would have joined the CDR regime who will no longer need to.

For example, under a closed CDR regime an accountancy software company would have become accredited to develop safe and secure CDR apps or piece of software that could assist accountants or financial counsellors in their work. But allowing CDR data to be disclosed to non-accredited parties undermines the incentive for the accountancy software company to become accredited and develop safe software. Why would they when they can continue to produce their existing software that the accountant could plug in the CDR data they obtain?

Implementing a closed system and preventing non-accredited parties to obtain CDR data free from obligations will encourage greater involvement in the CDR regime and will actually encourage the development of tools and apps in the CDR environment for those professions (identified in the consultation paper) to use.

Voluntary consent is undermined

The consultation proposes that the rules will:

> *require the ADR to ask for the consumer's consent to disclose their CDR data to a non-accredited person separately from the initial consent to collect and use their CDR data.*[36]

Putting aside the fact that the concept of consent will be stripped of all meaning by the complexity being introduced by the breadth of the proposals (see above), asking for consent to hand over CDR data to a non-accredited party is almost meaningless.

In reality most people who rightly (or wrongly) trust their advisor will simply do what the so-called trusted advisor will ask of them to do – be they their accountant asking to sign up and consent to providing them with their financial details or their lawyer.

The consultation paper states that:

> *We anticipate that disclosures of this kind are likely to occur in the context of an established commercial relationship between the ADR and the non-accredited person. For example, an accountant may recommend services of a particular ADR, or the ADR may identify accountants the consumer may use and transfer their CDR data to. This context provides*

[36] ACCC Consultation Paper Page 29

incentives for ensuring good consumer experience and trust and to mitigate the risk of reputational damage arising from unauthorised disclosure of data.[37]

We strongly disagree with this. Consumers are likely to simply "trust" their advisor and do what they ask. The context outlined does not provide incentives for good consumer experiences. Consent in this situation will be equivalent to the iTunes Agreement process where the consumer is highly likely to not engage with the details and simply go through the motions at the request of the non-accredited party. There is the very real possibility that consumers will be pressured into providing their consent. The consent here will be a fig leaf and place all the risk back on to the unsuspecting consumer. Consent here will neither be voluntary nor informed.

It is preferable that the ADR not simply provide a service to hand over data – but that it provide a service that assists the listed professions to handle the CDR data in a safe and secure environment. The listed professions should also be engaging with the accreditation process to create such services to compete in a safe and secure environment, or working with FinTechs to provide such a service to them.

The reputational damage incentive mentioned above is also a fiction. If reputational damage were truly an incentive then "trusted advisors" would seek to meet the safety and security requirements of the CDR in order to protect the interests of their clients. The steady stream of high profile data breaches from those in the financial services sector including RI Advice Group[38] Visa Europe Ltd and isignthis[39], PayID, [40] to Equifax,[41] MYOB,[42] NAB,[43] the list goes on and on and on.[44]

The only reputational damage that is likely to occur is the reputational damage to the CDR regime when the first breach of CDR occurs via a non-accredited party.

---

[37] ACCC Consultation Paper Page 29

[38] IT News ASIC sues financial services company for repeated hacks, August 2020 https://www.itnews.com.au/news/asic-sues-financial-services-company-for-repeated-hacks-552124

[39] iSignthis Ltd (ASX:ISX) Visa Europe Ltd -Breach of Personal Data, Yahoofinance, 17 August 2020, https://au.finance.yahoo.com/news/isignthis-ltd-asx-isx-visa-202100430.html

[40] PayID breach sees customers' banking information hacked, https://www.news.com.au/finance/business/banking/westpacs-payid-breach-sees-customers-banking-information-hacked/news-story/08c3fb5bad5ee01463233ed669b33013

[41] Equifax hit with major pay out for data breach settlement, Techradar, 23 July 2019,Prohttps://www.techradar.com/au/news/equifax-to-pay-dollar700m-in-data-breach-settlement

[42] Australian workers' salaries exposed after MYOB glitch, Yahoo!finance, 8 July 2019 https://au.finance.yahoo.com/news/peoples-salaries-exposed-after-myob-glitch-005414328.html

[43] NAB reveals 13,000-person data breach at 6PM Friday, itnews 26 July 2019 https://www.itnews.com.au/news/nab-data-breach-hits-13000-customers-528757

[44] For a large list of data breaches in Australia see: https://www.webberinsurance.com.au/data-breaches-list

CDR Consumers will not understand the implications of consenting to disclosure of CDR Data, or a CDR Insight, to a recipient outside of the CDR

We agree with the Maddocks PIA that CDR Consumers will not understand the implications of consenting to disclosure of CDR Data, or a CDR Insight, to a recipient outside of the CDR. It is highly likely that in the vast majority of cases consumers will not know what the risks and consequences of sharing their data outside of the protections of the CDR regimes. It is not in the interests of industry to fully spell out these risks.

The PIA is considering recommending that:

> *the ACCC consider only allowing CDR Data and CDR Insights to be disclosed outside of the CDR Regime to APP entities, or to entities who agree to comply with the APPs as if they were an APP entity.*[45]

While this may limit the harm somewhat it does not address the core problem with the proposal – that is the additional Privacy safeguards and other important consumer protections (including the requirements under the accreditation process) created by the CDR to ensure a safe and secure, trusted data environment for consumers will still not be available to consumers who provide their CDR data to non-accredited parties – be it in an informed and voluntary manner or otherwise.

There are no additional restrictions placed on what non-accredited parties can subsequently do with CDR data once obtained

The consultation paper proposes no additional restrictions on what non-accredited parties can do with consumer's CDR data once obtained. The only restrictions in place are those under the current *Privacy Act* – that is the inadequate direct marketing rules under Australian Privacy Principle 7 (which, for example does not require express consent for the data to be used for direct marketing purposes), as well as weaker notification, consent, use and disclosure requirements and no effective restriction on the sale of customer data under APPs 3,4,5, 6 and 8.

The Open Banking Report recommended that the "the protections of the Australian Privacy Principles should be modified in Open Banking to strengthen customer confidence."[46] The strengthened privacy safeguards were subsequently introduced. However this proposal subverts this intention meaning that it is business as usual in terms of poor privacy standards. Why bother developing the CDR at all?

[45] Maddocks PIA, Page 66

[46] Treasury, Open Banking, December 2017, Page ix, https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking-_For-web-1.pdf

The proposed mitigants will not deal with the risks

Requiring record keeping – while a good practice – does nothing to prevent harm from occurring in the first place and will simply assist in tracing the harm done after the fact, and assist in identifying liability.

The proposal also foresees the Data Standards Chair developing standards or guidelines including providing:

> *for example, warnings that the non-accredited person may not be subject to the Privacy Act 1988 (Cth).*[47]

Firstly these standards will only apply to the ADR not the non-accredited party where the safety and security threat lies.

Secondly the warning being used as an example is also next to useless given the likelihood of consumers simply doing what their "trusted advisor" tells them to do. If the advisor is "trusted" why wouldn't you do what they ask?

Thirdly 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.*[48]

While helpful for some, most consumer including those who "trust" their advisors and those experiencing financial hardship will be motivated to ignore the warnings. Financially vulnerable consumers for example will sign up to any service if they perceive they have 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 dodgy financial advisors, misbehaving mortgage brokers and private lawyers.

The result will be that the people who need increased consumer protections through the mishandling or misuse of sensitive financial data will inevitably be provided the fewest protections under the this proposal.

The high cost of accreditation should not outweigh the need for a safe and secure environment

Cost of accreditation as a barrier to entry has been raised as a reason why non-accredited parties such as accountants will be provided with the ability to obtain sensitive consumer data with no increased consumer protections.

Financial Rights view is that if accountants, mortgage brokers and other so-called trusted advisors are unable to afford providing a safe and security data environment for their clients

---

[47] ACCC Consultation Paper Page 29

[48] 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

then they do not and should not have an inherent right to access voluminous levels of sensitive financial data. This is why licensing requirements, best interest's duties and all other forms of regulation apply to these professions. Accessing this data is a new form of interaction and consumers must not simply rely on trust that their data will be handled appropriately – consumer protections afforded by the CDR must move with that data.

If a restaurant said that it would be too costly to implement an appropriately safe and secure food preparation environment – we wouldn't simply place all the risk back on the consumer by simply relying on consent. They wouldn't be allowed to vend.

We also note that the Maddocks PIA notes the following risk:

> *26. Risk relating to the transfer of CDR Data and CDR Insights to Trusted Advisers and Insight Recipients*

As we do not support Trusted Advisors obtaining CDR data we do think there is any value in exploring the way to mitigate the problems that arise when transferring such data when the data will still be held unsafely and insecurely by the non-accredited entities.

Disclosure of CDR insights to anyone

Another so-called limit to the leakage of a consumer's CDR data outside of the consumer protections afforded by the CDR regime is that "any person" may be provided with CDR data by a consumer but only in a so-called "CDR insight" form.

Financial Rights again strongly opposes the proposal to allow consumer's sensitive CDR data to leave the protections of the CDR regime by allowing the provision of "CDR insights".

On the surface this sounds like it is protecting consumers by decreasing the amount of data down to mere "insights" into that data. In fact the risks are exponentially worse.

Consumer insights are more sensitive than raw data

Sharing a consumer insight is as invasive, if not more invasive than, sharing the raw data of a consumer's CDR Data. This is because the "insights" are the value in the data and allows others to do away with the process of analysis.

The consumer insights proposal places all the responsibility on the consumer

The consultation paper acknowledges the riskiness of insights when it says they "may still be highly sensitive to an individual" [49] but then only plans to mitigate this huge risk by introducing some transparency to the process. In other words the proposal relies on disclosure whereby placing all the responsibility on the consumer to understand, and comprehend the potential risks involved – in the face of other competing demands including pressures to hand over the insights. This is unrealistic and does little to nothing to protect consumers.

[49] ACCC Consultation Paper, Page 30

Consumers will not have the automatic right to know what the insights are

But even when relying on disclosure as the sole risk mitigation strategy – the disclosure is limited to

> *require[ing] an ADR to record when an insight was disclosed and to whom, and enable a consumer to request records of each insight disclosed by the ADR but, mindful of the overall cognitive load of the CDR consent process for consumers, the proposed rules do not require additional information to be incorporated into consent.*[50]

In other words, consumer will not be automatically provided with the actual insights and will need to take the active step to request this information – information which is essential for people when challenging an adverse decision based on these insights.

We note that Proposed Rule 1.14(3)(ea) means that the consumer dashboard needs only list the consents to provide insight data and to whom the CDR data was disclosed and when – it does not include what the insight is.

But even if consumers were to be given the automatic right to see these insights – it is not entirely clear how a consumer is expected to understand the risks that such an insight if breached, accessed and used by other parties and how that is meant to lead to more informed decision-making. Again all of the responsibility and liabilities rest with the consumer.

Disclosure and increased transparency is not a solution here. As ASIC have outlined:

- Disclosure does not solve the complexity in financial services markets
- Disclosure must compete for consumer attention …
- In the real world, disclosure can backfire in unexpected ways[51]

What is required is a set of consumer protections that are built into the very structure of the model that incorporates privacy, security and safety into the design of the regime. This proposal is antithetical to this "privacy by design" approach.

Consent from vulnerable consumers is unlikely to be free or fully informed

All of the above problems is exacerbated when there is a consumer who is experiencing a form of vulnerability including but not limited to financial hardship or language difficulties that mean that they are less likely to full understand the nature of the request to consent to insight data being disclosed nor are in a position to necessarily say no to a request when there may be undue pressure placed on them and an incentive on their part not to inquire too deeply. Disclosure and transparency are particularly unlikely to assist vulnerable consumers.

---

[50] ACCC Consultation Paper, Page 30

[51] ASIC, 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

We therefore agree with the Maddocks PIA that here is a risk that an Insight Disclosure Consent from a vulnerable CDR Consumer may not be free and fully-informed[52] and that the ACCC must consider whether it is at all appropriate for CDR Insights to be part of the CDR Regime.

Accredited persons do not have to comply with the CDR rules when transferring an insight

This increases the risks inherent in such transfers including loss, breaches or other unauthorised access.

***

We note that the Maddocks PIA is considering recommending that

> *the ACCC consider whether it is appropriate for CDR Insights to be generated and disclosed as part of the CDR Regime. This is because of the inherent risks associated with the disclosure of the results of the analysis of raw CDR Data[53].*

We strongly agree with this and recommend that the ACCC drop this proposal immediately.

We note that Maddocks suggests as an alternative that

> *if the ACCC determines that it is appropriate for CDR Insights to remain within the scope of the CDR Regime, [we are considering recommending] implementing mechanisms to ensure that vulnerable CDR Consumers are giving free and fully-informed Insight Disclosure Consents.*

We do not support this potential recommendation because it is so vague that it is meaningless. Effective mitigants must be clearly spelt out and demonstrate genuine risk mitigation.

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.

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.

Anything less will increase the risk of harm to consumers exponentially and lay the grounds for the failure of the CDR once trust is undermined.

It is in the interests of all CDR participants – data holders, accredited parties and consumers to oppose this deeply flawed proposal.

---

[52] Maddocks PIA, Page 34

[53] Maddocks PIA page 67

Recommendations

5. **Financial Rights opposes the ACCC's proposal to facilitate the disclosure of highly sensitive financial information relating to CDR Consumers to non-accredited persons without appropriate measures to protect the privacy, safety and security of consumers.**
6. **The ACCC must go back to the drawing board and design develop a model for sharing of CDR data to new parties based on privacy-by-design and the following principles:**
    a. **consumers who choose to use and pass on their CDR data are afforded all the privacy and consumer protections under the CDR regime no matter who holds them;**
    b. **only accredited parties should be able to access and handle CDR data;**
    c. **all those who access and handle CDR must be required to meet high standards of security and safety as currently required under accreditation.**
7. **Any increased access to CDR data by interested parties that are not accredited should not even be considered until the *Privacy Act* has been reviewed (as recommended by the ACCC's Digital Platforms Inquiry) and increased consumer protections regarding the handling of data are increased as is the case in UK and Europe.**

Proposed changes to joint accounts

It is critical that the CDR regime account for vulnerable people in the handling of joint account information. Economic abuse and family or domestic violence can be perpetrated using financial services.

Financial abuse and harm can take many forms. It can involve elder abuse, domestic or family violence, and can happen over an extended period of time. It could include spending money without permission, accessing finances like early release superannuation payments, forging signatures, coercing someone to sign something, pension-skimming; using the person's bank account or credit card without their consent; denying them access to their money or bank statements, or opening and closing account to benefit one party over another. It can also involve a loan that is never paid back, threatening or pressuring someone to invest in something on their behalf, or forcing someone to provide services without being paid or fairly compensated, or expects you to pay their expenses. It can also involve the use or misuse of joint account information particularly in terms of granting one account holder information relating to the other account holder which can lead to the threat of physical violence. Financial abuse unfortunately materialises in multiple and ever shifting forms

It is therefore vital to ensure that:

- people 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.

While the proposal takes some steps in the right direction there remains much to be done to address the risks and threats that abound in this space. As such Financial Rights would not be able to support the proposal unless further work is undertaken on the proposal to mitigate these risks.

In the absence of a physical or financial harm or abuse flag, there is a risk that JAH A will simply pressure JAH B to agree to the disclosure of joint account information

Under the proposal when Joint Account Holder (**JAH**) A selects a disclosure option in the Joint Account Management System (**JAMS**), the Data Holder must notify JAH B that JAH A has selected a disclosure option and invite JAH B to select a corresponding disclosure option in JAMS. The notification includes a range of information including what the CDR is; that the disclosure option has been selected by JAH A and no disclosure would take place until the JAH B selects the same option as JAH A.

If there are no physical or financial harm or abuse flags in place held by a Data Holder, then there is the risk that a perpetrator JAH A may be able to simply force JAH B to agree to the request to

disclose, or agree on their behalf. This is common occurrence where there is a power imbalance or threat of physical violence.

The safety/privacy mechanism is therefore dependent on the Data Holder having a flag in place. This is not guaranteed.

It is not guaranteed in the situation where a perpetrator's first act of abuse is to use the CDR to benefit themselves and harm the other party.

It is not guaranteed in the situation where Data Holder has not been made aware of a threat, has not recognised and identified the threat themselves, or there is no means in place for a Data Holder to be made aware of the threat – i.e. where there is no way for the abuse victim to contact the entity, are not encouraged to do so or the Data Holder has no means to record or identify such a threat where such a threat is clear.

Currently, most banks and other lending do have contact forms, phone lines or other means by which a consumer can contact them to inform them. There are other more proactive means to identify financial abuse – many of which are currently being considered by banks in the ABA[54]

However it is our understanding that there is no requirement under the rules (or standards) for an accredited CDR participant in their subsequent role as data holder (or any CDR participant for that matter) to have a contact form which can be used by a customer to inform them of the situation. Nor is there any other requirement for functionality to flag physical or financial harm or abuse.

Not all accredited person will have existing processes in place – some may not be planning on introducing processes to assist in allowing people to contact them. Consumers already regularly find it difficult to get in contact with the makers of Apps, digital services and other software – with no phone numbers and in some cases no emails – or if they are there they may be difficult to find or not answered quickly.

How is the data holder going to be able to invoke the CDR rules re: the threat of physical or financial harm or abuse, if they don't know about it and how will they know about it if there isn't a requirement for a contact form to enable one joint holder to inform them or a requirement to proactively identify an issue.

At the very least for the mooted protections for vulnerable people to succeed the CDR needs to require of Data Holders (and Accredited Parties and Person) to establish the means by which those experiencing abuse or threats can alert Data Holders (and Accredited Parties and Persons) to this threat.

In recommending this we do so acknowledging that this is not the full solution of this problem since it relied on the ability of vulnerable consumers to confirm or self-disclose abuse – something that is not always possible in difficult, violent or coercive relationships.

That is why we also recommend that there are obligations on CDR participants to proactively identify such threats using analysis that is being used in some parts of the financial services sector. We acknowledge that there is likely to be insufficient cultural and technical capacity

[54] see: https://www.ausbanking.org.au/raising-the-bar-to-help-customers-doing-it-tough/)

within Fintechs to recognise and accommodate such disclosures and to develop and apply any protocol for implementation of associated safeguards. However, both requirements recommended above are critical if vulnerable consumers are to be protected from threats, abuse and harm inherent in the CDR regime.

The requirement to share without the approval of JAH B (in order to prevent physical or financial harm or abuse to JAH A) assumes that there is a process or policy that enables a data holder to learn of such a threat

In the case where JAH B is the perpetrator and JAH A is fleeing a situation or seeking options to assist themselves, the proposal again falls over on the lack of any requirement for the CDR participants to have procedures in place to be informed of such a threat or proactively identify such threats.

The proposal only applies to Data Holders - ADRs or APs are not required to give a joint account holder control over their data at this stage of the process.

Financial Rights agrees with the risk identified by the Maddocks PIA that

> *"The CDR Rules are currently silent on whether disclosure options must be selected (or confirmed) before an Accredited Data Recipient (or Accredited Person) may disclose CDR Data on a joint account to another Accredited Person, a Trusted Advisor or an Insight Recipient (noting that this would be a CDR Insight based on raw CDR Data relating to a joint account).*
>
> *In other words, there is currently no mechanisms for JAHs to consent to the disclosure of joint account data once it is held by the Accredited Data Recipient. This means that JAHs have no control over their joint account data at this stage.*[55]

Further work is required here.

There may be inconsistency between an online and an offline JAMS

Again Financial Rights agrees with the risk identified by the Maddocks PIA that:

> *there will be an ability for CDR consumers to select a disclosure option in an 'offline' version of JAMS, [and] there is a lack of clarity about how data holders will be required to ensure that they accurately and promptly reflect the offline selection in their online version of JAMS. This raises the privacy risk that a disclosure option selected in the offline version will not be properly implemented in the online version of JAMS, which is relied upon for processing disclosures of joint account CDR Data.*[56]

Further work is required here.

[55] Maddocks PIA page 80

[56] Maddocks PIA page 83

There is the threat that JAHs will not understand the consequences of selecting a disclosure option in the JAMs even with the information provided.

Again - as with many of the proposals being put forward – combination of:

- the complexities involved in the consent process,
- the complicated financial and privacy concepts involved;
- the likely lack of experience with the system and
- the likelihood of a disinterested JAH skimming or an interested JAH being pressured to agree to a disclosure request

means that JAHs will not understand the consequences of selecting a disclosure option in the JAMs even with the requirement for information to be provided.

The current proposal's over-reliance on disclosure in lieu of structural protections built in to the CDR through the privacy by design process means that the proposals being put forward with respect to joint accounts has the potential to undermine informed and voluntary nature of consent and lead to consumer harms.

There is no clear and standardised level of evidence or guidance if an exception to the JAMS is to apply

Again Financial Rights agrees with the risk identified by the Maddocks PIA that:

> *the proposed amendments to the CDR Rules do not oblige the Data Holder to require a particular, clear and standardised level of evidence, if an exception to the JAMS election process is to apply.*[57]

While we agree with Maddocks that:

> *the CDR Rules [should] prescribe the level of evidence that a Data Holder must be satisfied of before determining that an exception to the disclosure option process in JAMS is to apply (or that a notification need not be given).*[58]

the standards developed should be such that they do not inadvertently act as a hurdle or roadblock to a CDR consumer subject to the threat of harm or abuse, cannot obtain such protections.

[57] Maddocks PIA, Page 84

[58] Maddocks PIA, Page 84

Recommendations

8. Financial Rights cannot support the current proposals for joint accounts unless further work is undertaken to mitigate the risks including:
    a. requiring all CDR participants to provide easily accessible and obvious means for consumers to inform CDR participants of the threat of physical or financial harm or abuse,
    b. requiring all CDR participants to proactively identify such threats using analysis or other means.

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 Drew MacRae, Policy and Advocacy Officer, Financial Rights on [redacted].

Kind Regards,

[redacted]

Alexandra Kelly
Director of Casework
Financial Rights Legal Centre