Financial Rights LEGAL CENTRE

Submission by the

Financial Rights Legal Centre

Australian Competition and Consumer Commission

Consumer Data Right Rules Framework, September 2018

October 2018

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 close to 25,000 calls for advice or assistance during the 2017/2018 financial year.

Financial Rights also conducts research and collects data from our extensive contact with consumers and the legal consumer protection framework to lobby for changes to law and industry practice for the benefit of consumers. We also provide extensive web-based resources, other education resources, workshops, presentations and media comment.

This submission is an example of how CLCs utilise the expertise gained from their client work and help give voice to their clients' experiences to contribute to improving laws and legal processes and prevent some problems from arising altogether.

For Financial Rights Legal Centre submissions and publications go to
www.financialrights.org.au/submission/ or www.financialrights.org.au/publication/

Or sign up to our E-flyer at www.financialrights.org.au

National Debt Helpline 1800 007 007
Insurance Law Service 1300 663 464
Mob Strong Debt Help 1800 808 488

Monday – Friday 9.30am-4.30pm

Introduction

Thank you for the opportunity to comment on the Australian Competition and Consumer Commission's (**ACCC**) Consumer Data Right (**CDR**) Rules Framework.

The Financial Rights Legal Centre (**Financial Rights**) continues to take the view that the Consumer Data Right as materialised in the *Treasury Laws Amendment (Consumer Data Right) Bill 2018* is fundamentally misconceived and is:

- limited in scope and misleads consumers;
- piecemeal and entrenches Australia falling behind the rest of the world;
- establishes multiple privacy standards, confusing consumers and placing them at risk;
- facilitates the leakage of sensitive financial data to entities that provide lower privacy protections;
- establishes flawed and incomplete privacy safeguards; and
- cements in place two very different FinTech sectors

While the approach being taken by Treasury may be appropriate for developing consistent application programming interfaces (**APIs**) and data standards for vastly different sectors of the economy and their unique data sets[1] , it fails to effectively address standard privacy and security expectations that apply equally across the economy.

By taking this approach the CDR regime creates a new set of strengthened privacy safeguards that will only apply to certain designated sets of financial data in certain limited circumstances. Over time it is expected that this will expand to cover certain other sectors in further limited circumstances. This approach in providing privacy safeguards for sensitive data use is therefore by its nature, limited and piecemeal.

The approach also stands in stark contrast with the European Union (**EU**). The EU have taken strong strides into bolstering consumer protections in this space with the new General Data Protection Regulation (**GDPR**) from May 2018 and the Payment Services Directive 2 (**PDS2**) coming into force early this year in January 2018.

The full expression of Financial Right's position is in our submission on the draft *Treasury Laws Amendment (Consumer Data Right) Bill 2018* available on our website.[2]

Notwithstanding this, Financial Rights wishes to approach the creation of a Consumer Data Right Rules Framework constructively.

---

[1] banking and financial information versus energy, telecommunications, social media, insurance and other sectors yet to be identified

[2] http://financialrights.org.au/wp-content/uploads/2018/09/180907_CDRLegislation_Submission_FINAL.pdf

While much of the design of the CDR legislation as proposed by Treasury will be relevant for any discussion of the proposed ACCC CDR Rules framework, our comment will be limited to the Rules Framework being proposed.

Sharing Data with Third Parties

Financial Rights generally supports the ACCC proposal to make rules to the effect that:

- An accredited data recipient may only collect and use a consumer's data where it has obtained their consent, and only in accordance with that consent.
- A data holder must share a consumer's data with an accredited data recipient where the consumer directs and authorises the data holder to do so.
- Data sharing must only occur where the consumer has given relevant informed consent to the accredited data recipient and authorisation to the data holder.
- Authorisation and authentication processes will meet certain requirements.
- Data sharing must occur via an API. The API will be implemented in accordance with the standards developed by the Data Standards Body, and data sharing must occur in accordance with those standards.

Financial Rights also supports the ACCC proposal that data sharing will not be subject to fees. We note that this is planned to be the case for at least the first iteration of the rules.

Charging a fee to access your own personal information under the CDR would be a significant barrier to access. For particularly vulnerable consumers experiencing significant financial hardship, any fee, no matter how small it seems to others, will be too much and act as a barrier to such access. Introducing a fee under the rules would embed a class system for accessing one's personal information. Even if a waiver were to be made available, this would be an additional hurdle to a cohort of consumers who, based on past experience, will simply not take the steps required.

We note that the current APP 12 states that an organisation may charge an individual but that it must not be excessive and must not apply to the making of the request. This needs to be fundamentally reconsidered in a review of the Australian Privacy Principles (**APPs**) and the *Privacy Act*.

With respect to any consideration of a fee for value added data or derived data in the future, it needs to be remembered that while a data holder may have added value to the data via some form of analysis – it still remains the consumer's personal information. If it wasn't, such data would hold little to no value at all. Consumers should retain the right to their data despite work being done to it through analysis, and should be able to access this data for free.

Recommendations

1. **Consumers should retain the right to their data including derived or value added data for free.**

CDR consumer – who may take advantage of the CDR?

The ACCC proposes that the first version of the rules will enable a consumer to direct a bank to share their data only if they are currently a customer of that bank.

Financial Rights believes that this is a reasonable first step and accepts the challenges outlined by the ACCC include authenticating former customers. We do however support their inclusion at some stage but understand that it is not critical for the development of the first set of rules.

The ACCC proposes that the first version of the rules extend the CDR to consumers who have access to and use online banking, but not to offline consumers.

The ACCC seeks stakeholder views on what would be a reasonable timeframe for extending the CDR to former customers and offline consumers.

While Financial Rights understands and accepts why the ACCC would choose not to include those consumers who do not have access to online banking as a part of the first iteration of rules – given the tight timeframes involved – we would however wish to avoid the Rules acting to further embed a digital divide through the absence of offline consumer provisions.

Financial Rights notes that there are a significant number of Australians who do not have access to online banking. There also remains significant numbers of Australians who do not have access to the internet: 1.3 million households as of 2015. Many of these people are disadvantaged, lack confidence or knowledge to access the internet or unable to afford access. Providing them with access to Open Banking could potentially empower many of these Australians but could also potentially open up come of the most vulnerable Australians to unscrupulous behaviour and exploitation.

Consequently we would want to see specific protections and security measures included in the rules for offline customers to avoid potential elder abuse, misuse or other unscrupulous behaviour. While Financial Rights has no strong view on a time frame – indeed a longer timeframe could potentially protect vulnerable customers (financially or otherwise) from any problems that arise from the implementation of the CDR - we would want comprehensive consideration of these issues to be prioritised for a second iteration of the Code.

Recommendation

2. **Access to CDR should be provided to those without online banking access. Specific additional protection and security measures should be included here to avoid potential elder abuse, misuse or other unscrupulous behaviour.**

Accreditation

The ACCC proposes to provide for a single general tier of accreditation in the first version of the rules.

The ACCC also supports the development of lower tiers of accreditation, and welcomes the views of stakeholders about the tiers that it would be practical to implement and the basis for any reduced accreditation requirements.

Financial Rights supports the development of lower tiers of accreditation but believes that this must form a part of the first version of the rules.

While again, we understand the tight timeframes involved, accrediting intermediaries as conceived by the ACCC is critical to ensure that consumers are not, from the beginning subject to any lower security or privacy protections via the leakage of CDR data to non-accredited parties.

If these lower tiers are not to be a part of the first version of the rules, there should be a prohibition on any non-accredited party accessing CDR data until there is.

Our key concern is that the introduction of the CDR regime as currently conceived will create multiple levels of privacy standards that will apply at different times to consumers seeking protection, security and redress when something goes wrong. They include:

- CDR Privacy Safeguards as envisioned under this draft legislation – essentially strengthened versions of the 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.

To demonstrate the complexity of what is being proposed by the draft CDR legislation, a consumer could potentially be subject to the following array of high and low protections:

1. Transactional data held by a bank that may at some point in the future be CDR data (a data holder) but has yet to be requested to be ported, is currently and will continue to be subject to the APPs.
2. This transaction data becomes "CDR data" once requested to be transferred to an accredited Data Participant where its transfer and use will be subject to the CDR Privacy Safeguards.
3. The transactional data continuing to be held by the original bank remains subject to the APPs.
4. CDR data collected and held by an accredited Data Participant will be subject to the CDR Privacy Safeguards.
5. Non-CDR Data held by Accredited CDR Participant small businesses will be subject to the APPs (as reformed by proposed Subsection 6E(1D) of the *Privacy Act*)
6. CDR data held by non-accredited parties who are "APP entities"[3] will be subject to the APPs, not the CDR privacy safeguards.
7. CDR data 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.

This has been confused even further by the second stage of Treasury proposals for the CDR which seeks to "clarify" the interaction of the Privacy Safeguards and the *Privacy Act*:[4]

[3] 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

[4] https://treasury.gov.au/consultation/c2018-t329327/

Application of Privacy Safeguards by CDR participant

CDR Participant	*Privacy Safeguard that applies*
Data holder	PS 1 – Applies concurrently to APP 1 PS 10 - Applies to the disclosure of CDR data and there is no similar requirement under the Privacy Act PS 11, PS 13 – Apply to the disclosure of CDR data and substitutes for APPs 11 and 12 in respect of disclosed CDR data
Accredited person	PS 1, PS 3, PS 4, PS 5 - The APPs apply concurrently, but with the more specific Privacy Safeguards prevailing.
Accredited data recipient	PS 2, PS 6, PS 7, PS 8 , PS 9, PS 10, PS 11 – The Privacy Safeguards apply and substitute for the APPs. The APPs do not apply to an accredited data recipient of CDR data in relation to the CDR data that has been received or data derived from that data.

This proposed schema above is, on the face of it, complex and a potential nightmare for both industry and consumers alike. How anyone (including lawyers) is supposed to navigate the proposed application of privacy safeguards is beyond us.

The introduction of the concept of providing non-accredited CDR participants the ability to access CDR against the recommendation of the Open Banking Report provides a significant leakage point for CDR data to fall outside of the system, whereby consumers will, at a minimum, 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.

In fact, the draft CDR legislation is designed to encourage consumers to engage with the CDR regime with the promise of increased protections, all the while allowing this data to leak out of the CDR regime to where lower or no privacy standards at all apply. In other words, the draft CDR legislation will facilitate incredibly sensitive financial and personal data to be handled by non-accredited parties with lower or no protection for consumers.

This is unacceptable.

We accept that the government has not committed to reviewing the *Privacy Act* and the APPs to provide strengthened privacy protections for Australians in a modern 21st century data driven economy.

However a simple solution to this issue would be to create lower forms of accreditation to ensure that those entities such as accountants are able to access the CDR and ensure that

consumers are still provided with the necessary privacy and security protections required for handling CDR data.

The scenario listed under 12.1.1 currently has a consumer wishing to have their CDR data disclosed to a non-accredited entity like an accountant for the preparation of a tax return. The ACCC proposes to make rules requiring accredited data recipients to transfer data to a non-accredited entity if directed by a consumer to do so (with their express consent) and ensuring that the consumer is notified that:

- the entity they are sending their data to is not accredited under the CDR and therefore the CDR protections no longer apply
- the non-accredited entity's handling of their data may be covered by the *Privacy Act*
- disclosure is at the consumer's own risk.

We cannot support this proposal.

Firstly, how will a consumer be expected to understand what is meant by being subjected to CDR privacy safeguards, the *Privacy Act*, the APPs or none of the above? Even if the consumer was told explicitly what the arrangement was, how is the consumer expected to know that the *Privacy Act* and APPs are weaker forms of protection to the CDR privacy safeguards, and not very effective privacy protections? Will these higher, lower and lowest forms of protection be made explicit to consumers? And if these higher, lower and lowest forms of protection are made explicit, will it even change a consumer's behaviour? At the very least this would need to be consumer tested for effectiveness. Reliance on mere disclosure will do little to empower a consumer in this situation.

Second, what will prevent a consumer from signing up for a service that will include data handled by a non-accredited party, where there is a willingness on the consumer's part to sign up to anything, even with lower privacy standards. Financially vulnerable consumers will sign up to any service if they are desperate enough, or perceive no real choice. Financial Rights knows from its work on the National Debt Helpline that many Australian consumers are vulnerable to the promises of debt management firms, quick-cash payday lenders, and online companies that promise to solve all of their financial problems for a fee or in exchange for their personal information.

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

Consequently, the people who are most in need of protection – the financially vulnerable - will inevitably be provided the fewest protections under the ACCC proposal and the CDR regime.

It has been argued at ACCC consultations that such data is already being provided to accountants and other entities without greater protections. Our response to this is (a) consumers need greater protections in these circumstances and simply because that is the way it is now doesn't mean reform is not urgently required and (b) this will be a reputational risk to the CDR regime – it is CDR data. Any problems that arise from here on in will be blamed on the CDR regime and confidence and trust will be undermined when problems inevitably arise.

Financial Rights asserts that it is within the power of the ACCC to take another course.

We believe that the ACCC needs to introduce a form of lower accreditation for entities that would fall under the scenario at 12.1.1. That is entities who are not expected to be data recipients in the sense originally conceived under the Open Banking Report – ie not a FinTech, but an entity who may be acting on behalf of a consumer in a representative capacity or interacting with a consumer in some form where access to CDR data is desired or required. These include:

- accountants
- financial advisors
- insurance brokers
- mortgage brokers
- debt management firms
- debt collectors
- pay day loan and consumer lease operators
- real estate agents
- landlords
- book-up providers

Generally speaking any sole trader or small businesses who provides "middleman" or advice services are likely to seek to gain access to CDR data and will not be in a position (financially or otherwise) to become an accredited party as foreseen under the draft legislation and EDEM. Nor will they be incentivised to be an accredited member.

We therefore believe that the ACCC needs to re-think the scenario at 12.1.1 to develop a category of lower tier accreditation to capture the scenarios described above – scenarios we suggest are likely to be very common and easily understood and identified.

To repeat, if a lower tier category of accreditation is not created, the CDR regime proposed will be allowing the leakage of incredibly sensitive personal data to entities who provide significantly lower privacy and security protections.

It is the resolution of this one single issue that we predict will be the make or break the CDR regime. The CDR's success or failure rests on this since any abuse, exploitation or problems that arise from the misuse or breach of data by a non-accredited party will destroy any consumer confidence or trust in the CDR regime.

Financial Rights appreciates the challenge that ACCC has been left with in solving this problem – a problem that could be addressed by boosting consumer privacy protections more broadly - but we believe that the power lies with the ACCC to resolve the issue through this one simple fix.

Recommendations

3. Financial Rights supports the development of lower tiers of accreditation but believes that this must form a part of the first version of the rules.
4. If lower tiers are not to be a part of the first version of the rules, there should be a prohibition on any non-accredited party accessing CDR data until there are rules creating lower tier accreditation.
5. Financial Rights does not support the ACCC proposal outlined at 12.1.1. The ACCC must introduce a form of lower accreditation for entities who would fall under this scenario, i.e. entities who may be acting on behalf of a consumer in a representative capacity or interacting with a consumer in some form where access to CDR data is desired or required.

The ACCC proposes to make rules that the Data Recipient Accreditor grant accreditation to an applicant if it is satisfied that:

- **the applicant is a 'fit and proper' person to receive CDR data**
- **the applicant has appropriate and proportionate systems, resources and procedures in place to comply with the legislation, the rules and the standards including in relation to information security**
- **the applicant's internal dispute resolution processes meet the requirements specified in the rules and the applicant is a member of an external dispute resolution body recognised by the ACCC**
- **the applicant holds appropriate insurance. The ACCC welcomes views about appropriate insurance cover, current availability and cost.**

Financial Rights strongly supports the ACC's proposal.

The ACCC proposes to make rules that will specify the manner in which accredited data recipients are permitted to describe their accredited status.

Financial Rights supports the ACCC basing its rules with respect to Accreditation status disclosure on the UK Financial Conduct Authority (**FCA**) rules.

The ACCC does not propose to provide for recognition of accreditation in other jurisdictions in the first version of the rules.

Financial Rights supports this proposal.

The ACCC proposes to make rules that will require any foreign entity that is granted accreditation to appoint a local agent that will be responsible for any obligations of the foreign entity under the CDR regime.

Financial Rights supports this proposal.

The ACCC proposes to make rules specifying the powers and obligations of the Data Recipient Accreditor, including rules:

- **allowing the Data Recipient Accreditor to suspend or revoke an accredited data recipient's accreditation on grounds relating to the criteria for accreditation and to protect the security or integrity of the CDR regime**
- **providing for the revocation of accreditation where this is requested by an accredited data recipient.**

Financial Rights supports these proposals but wishes to suggest that the Data Recipient Accreditor may suspend or revoke an accredited data recipient's accreditation where civil proceedings are commenced alleging a contravention of discrimination laws. While these may be a "serious offence" as referred to in the Framework paper we think that this should be referred to specifically. This arises from our genuine concern for discrimination to arise through the use of algorithms and black box technologies that embed implicit biases and discriminate against particular groups of Australian consumers in some form.

Recommendations

6. **Data Recipient Accreditor revocation or suspension rules should explicitly reference discrimination laws.**

The ACCC proposes to make rules that will specify what happens in relation to a data recipient's CDR obligations when a decision is made to suspend or revoke its accreditation.

The ACCC proposes to make rules that will require an accredited data recipient that enters into an outsourcing arrangement involving the disclosure of CDR data to ensure it has appropriate plans and processes in place for managing risk.

Financial Rights supports these proposals.

The Register

The ACCC proposes to make rules relating to the Register, including in relation to the information required to be made publically available online and the powers and obligations of the Accreditation Registrar.

Financial Rights support this proposal. We believe that the register must be made public and in a format that is accessible to consumers, not simply kept on a regulator's website that no-one will ever access.

Consent

The ACCC proposes to make rules to the effect that where consumers with a joint account hold individual authority to transact on that account they will each be able to give individual consent to share their joint data under the CDR regime. The rules may require that each joint account holder be notified of any data sharing arrangements and given the ability to terminate them should they wish.

Financial Rights generally supports the recommendation to ensure that each joint account holder be notified of any data transfer arrangement initiated on their accounts and given the ability to readily terminate any data sharing arrangements initiated by any other joint account holders.

However as alluded to in the Framework paper, we have concerns that this may be problematic in a domestic or family violence context. We believe that any rules established should be designed with these issues in mind.

As the Economic Abuse Reference Group (**EARG**) states:

> *Family violence can have a significant detrimental impact on a woman's financial wellbeing, both during the violent relationship, and if (and when) a woman leaves the perpetrator. Financial insecurity is one reason a woman may stay in a violent relationship. Leaving a violent relationship must sometimes be done quickly and suddenly. A woman may not be able to take much with her, or may have to move far away from her home due to safety concerns. This can leave a family violence survivor (and often her children) with few financial resources and make it difficult to find secure housing and establish a new life.*[5]

Economic abuse as a form of family violence can exacerbate the situation faced by many women. Economic abuse can currently include, among other things, coercing a woman to:

[5] Economic Abuses Reference Group, Good Practice Industry Guideline for Addressing the Financial Impacts of Family Violence, version 1a, 4 April 2017, https://eargorgau.files.wordpress.com/2017/03/good-practice-guide-final-0404172.pdf

- incur debt for which she does not receive a benefit, or take on the whole debt of a relationship;
- relinquish control of her assets or income, or reduce or stop paid employment;
- claim social security payments;
- sign a contract, loan application or guarantee;
- sign documents to establish or operate a business;
- disclose her credit card details and/or passwords;
- provide cash;

or preventing a woman from:

- accessing joint financial assets, such as a joint bank account, for the purposes of meeting normal household expenses;
- accessing online banking or purchasing;
- seeking or keeping employment.

There may very well be potential problems arise out of the CDR regime as it applies to open banking. These could include:

- inadvertently alerting an abusive partners to financial related activity that places the abused partner in an unsafe position;
- conversely, preventing abused partners from accessing products and services that would assist their situation; and/or
- consents may not be freely given when consenting to use a product or service.

We recommend therefore that developing rules and standards with respect to joint accounts take into account the good practice principles developed by the EARG that ensure that safety and security are paramount.

Recommendation

7. **In developing CDR rules with respect to joint accounts, EARG's good practice principles must be considered to ensure that safety and security of those subject to family violence and economic abuse are paramount.**

The ACCC does not propose to make rules that would seek to treat minors differently from any other consumer who may take advantage of the CDR.

Financial Rights strongly disagrees with the ACCC's proposed approach to not make rules treating minors differently from any other consumers who may take advantage of the CDR.

Children are particularly vulnerable to the allure of new technology and new apps and may not fully understand the consequences of any consents required.

Their inclusion in the first iteration of the CDR is concerning since they will be the most vulnerable and at risk group arising from their inability to necessarily understand the full range of contractual obligations and subsequent consequences .

We note that the EU's GDPR restricts the ability to consent to those 16 years (or potentially 13 years and above) depending on the State. Article 8 states:

Art. 8 GDPR Conditions applicable to child's consent in relation to information society services

1. *Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.*
2. *The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.*

We also note that the ACCC have pointed to the fact that many minors are already able to transact on accounts without the consent of a parent or guardian and that there is no age limit under the APPs applying to consent. This however does not mean that nothing should be done. Just because the current rules don't treat minors differently does not mean that in the CDR should have the same rules. As noted we believe that minors are particularly vulnerable to exploitation and the risks versus potential benefits are high.

For example, the Dollarmites program run by Commonwealth Bank in schools received a SHONKY Award this year from CHOICE. The Dollarmites program works by offering commissions to primary schools in exchange for running the school banking scheme. The commissions include a one-off payment of $200 when the first student makes their initial deposit as well as annual rewards of up to $600 per year.[6] Recent investigations from Fairfax found that Commonwealth Bank staff fraudulently activated Dollarmite accounts for personal gain.[7]

We cannot see what would stop a bank, FinTech or any other data recipient from instigating similar marketing programs directed at children.

This is particularly a concern in the FinTech sector since technologies provide the ability for individual consumers to retreat into private, hidden, digital spaces to transact with FinTech providers. For example, a person who uses a pay day loan once will be targeted for more pay

[6] https://www.commbank.com.au/personal/kids/school-banking/information-for-schools.html?ei=bld2-btn-information-for-schools

[7] https://www.smh.com.au/business/banking-and-finance/dollarmites-bites-the-scandal-behind-the-commonwealth-bank-s-junior-savings-program-20180517-p4zfyr.html

day loans via the advertising on their browser as well as text, email or other forms of spam. Given the ease, speed and inherently private nature of applying for a new loan on an app, the usual social cues and hurdles that would work to potentially stop someone from accessing further predatory finance are simply no longer there. As someone falls further and further into the spiral of debt and shame, people will retreat further into the private sphere using their mobile phones away from other people (family and friends) only serving to exacerbate the problem over time.

These issues are exacerbated when we consider the use of phones by minors and a willingness to hide activities from guardians and parents.[8]

Data recipients should be required to demonstrate that they have verified someone's age and identity before acquiring consent to share CDR data. We recommend ACCC reach out to Youth Action NSW who has done advocacy on young person consent issues.

Recommendation

8. **Restrictions similar to Article 8 of the EU GPDR should be implemented with consent rules specific to minors considered.**

The ACCC proposes to make rules to the effect that an accredited data recipient must obtain a consumer's consent to both collecting, and using, specified data for specified purposes and for a specified time.

Financial Rights supports this proposal.

The ACCC proposes to make rules requiring consumer consent to be freely and voluntarily given, express, informed, specific as to purpose, time limited and easily withdrawn. In particular, the ACCC proposes to make rules to the effect that:

- **accredited data recipients cannot make consent to share data a precondition to obtaining other services not related to, or dependant on, the sharing of CDR data.**
- **consent must be unbundled with other directions, permissions, consents or agreements, and must not rely on default settings, pre-selected options, inactivity or silence.**

Financial Rights strongly supports the development of a consent regime that ensures that consent should be freely given by the consumer.

[8] Just as one example, Madhumita Murgia The secret lives of children and their phones, October 6, 2017 https://www.ft.com/content/7c972e2e-a88f-11e7-ab55-27219df83c97

We note that the ACCC proposes to make rules to the effect that consent should be voluntary in the sense described by the OAIC's APP guidelines, and must also be freely given as described in the current APP guidelines at B.43 and B.44, that is:

> *Consent is not voluntary where there is duress, coercion or pressure that could overpower the person's will. Factors relevant to deciding whether consent is voluntary include:*
>
> - *the alternatives open to the individual, if they choose not to consent;*
> - *the seriousness of any consequences if an individual refuses to consent; and*
> - *any adverse consequences for family members or associates of the individual if the individual refuses to consent.*

While this seems fair-minded we recommend that the ACCC expand upon these on these concepts in a similar way to the EU guidelines on consent.[9] These guidelines provide significant further details to the nature of many of the concepts inherent to consent and examine a multitude of situations and concepts to enable genuine consent to be effective. The guidance for example acknowledges that there are a number of situations where genuine consent cannot be freely given – for example in situations where there is a significant imbalance of power.

The EU guidelines' approach to consent is that it must be:

- freely given, absent of any element of inappropriate pressure or influence upon the consumer preventing them from exercising their free will including:
    - any imbalance of power;
    - the presence of any conditions via for example, the bundling of consent of necessary and unnecessary uses;
    - the conflation of several purposes without consent for each specific use; and/or
    - detriment to the consumer if consent is withdrawn or refused;
- specific including clear separation of information related to the obtaining of consent for different data processing activities;
- able to be constrained according to the customer's instructions including easily withdrawn with immediate effect and deletion of data;
- fully informed, transparent and fair,
- time limited; and
- an unambiguous indication of wishes via an affirmative act from the consumer.

While the ACCC proposal touches on many of these concepts such as unbundling some other concepts are not addressed.

[9] under Regulation 2016/679 as at 10 April 2018

An imbalance of power for example is a significant factor in whether a consent is freely given. Imbalances of power can arise from employment arrangements, dealings with authorities or where the consumer feels there is no choice but to agree. Any conditions placed upon a consent should be a factor considered as should any implicit or explicit detriment that could arise from withdrawal or from non-consent.

Recommendation

9. **ACCC rules for consent should be based on the EU consent guidelines Regulation 2016/679.**

- **accredited data recipients must provide specified information to consumers as part of the consent process.**
- **consent be obtained using language and/or visual aids and a process that is concise and easy for consumers to understand, and that, as part of the standards-setting process, the consent process should be tested for consumer comprehension. Accordingly, the ACCC does not propose to make a rule requiring all information to be displayed on a single screen.**

Financial Rights supports the list of specified information to be provided to consumers and importantly agrees that rules should be in place to require consent by obtained using is visual aids and that is concise and easy for consumers to understand. Proposed consumer comprehension testing of the consent process is critical here.

Importantly Financial Rights supports the ACCC proposal to not make a rule requiring all information to be displayed on a single screen. We agree that a single screen will not necessarily promote informed consent and meaningful engagement by consumers in and of itself.

Behavioural and consumer comprehension testing and design best practices should guide the way rather than a 'hunch' that a single screen will promote better engagement.

Friction in the consent process – ie minor impediments slowing the process such as multiple screens – is not necessarily a bad thing.

Consumers generally seek convenience and speed over security and suitable products. However there are many cases where they do so to their own detriment. Frictionless transactions are already causing significant consumer harm in the online consumer space, for example the ease of accessing payday loans via mobile applications. We also expect a large increase in complaints regarding the new PayID platform, due to the instant nature of transactions.

Some friction needs to be embedded into the Open Banking environment to enable better consumer decision making, particularly for harmful products.

While a single page sounds good in theory, we remain concerned that such brevity will be used to obfuscate the extent and nature of some of the uses being sought by the data recipient. We do not support the ongoing use of consents with extensive bundled terms and conditions that are used to hide all sorts of information and rely on inferred consent. Similarly we do not want the consent to be so short that Open Banking entities are forced to be necessarily broad and all-encompassing. This is the difference between detailing a page of multiple uses for the use of data for marketing versus a statement that asks the consumer to agree to 'all and every conceivable use from here until eternity.'

Consent should be straightforward, meaningful, informative and unable to be relied upon by data recipients where the ultimate use in dispute is not expressly described in the consents but is merely implied or captured in a broad catch-all phrase. The ultimate use of data should not surprise any consumer down the track. If it does there has been a problem at the consent stage.

If it is demonstrated via behavioural testing that greater comprehension is gained from a single screen we are willing to accept this but as the ACCC notes there is evidence to the contrary.

- **accredited data recipients must disclose, in an unambiguous way at the time of seeking the consumer's consent, the uses to which data will be put. Accredited data recipients may only use data in line with the uses to which the consumer has consented, and should only seek consent to access the minimum data necessary for the uses agreed to.**

Financial Rights supports this proposal.

- **the ACCC proposes to make a range of rules which will help provide consumers with a straightforward withdrawal process.**

Financial Rights supports this proposal.

The ACCC welcomes stakeholder views regarding the extent to which a consumer should be able to decide whether their redundant data is de-identified or destroyed.

Financial Rights view is that once an accredited data recipient has provided the service as agreed in a consumer's consent or where the accredited data recipient's accreditation is revoked then the data or redundant data must be automatically destroyed. This would embed a privacy-by-design approach into the CDR rules.

This would implement in part the EU's GDPR Article 17 which provides for the "Right to Erasure" where an individual will hold the right to request the erasure, *without undue delay*, of any links to, copy or replication of the data in question, under the circumstances where:

- the data is no longer necessary in relation to the purposes for which it was collected: Article 17(1)(a)

or

- the individual withdraws consent or the relevant storage period has expired and the data holder doesn't need to legally keep it (such as banking records for a seven year time period): Article 17(1)(b)

Consumers will have the reasonable expectation that once a consumer withdraws consent or their consent is expired, that their information will be deleted or destroyed in order to protect their privacy. This was acknowledged explicitly in the *Open Banking Report*:[10]

We note that there will be calls for entities to maintain data (be it in a de-identified or aggregated or amalgamated form). The argument here is that such data could assist the company to improve their products for others.

While such reasons may exist, we cannot see what the benefit is for the consumer. The consumer's data becoming essentially a commercial input into a business model without recompense.

If an accredited party has had their accreditation revoked – this would be for a serious breach. Why should consumers accept that a company that has had its accreditation revoked gets to hold on to the consumer's data (even in de-identified form) for any reason, commercial or otherwise. Surely they should have any and all privileges revoked at this point.

For those consumers who have left or ceased a service, there is very little incentive that we can see for them to agree to having their personal information held in any form, particularly given the inherent risks.

If a decision is made to allow de-identified data to be used in some form, then at a minimum this must be an express opt-in at the time of the ceasing of the service *and* rules de-identification would take an approach similar to that taken in the EU.

The EU GPDR law has focussed on the concepts of "anonymous data" and "pseudonymous data". The EU concept of "anonymous data" is only considered as such if re-identification is *impossible*, that is, re-identifying an individual is impossible by any party and by all means likely reasonably to be used in an attempt to re-identify.[11] Further, "pseudonymous data" is defined as

> *"the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information."*

The GPDR permits data holders to process anonymous data *and* pseudonymised data for uses beyond the purpose for which the data was originally collected.[12] Recitals 78 and Article 25 foresee pseudonymisation as a method to demonstrate compliance with Privacy by Design requirements, a concept we have recommended in previous submissions and continue to do so.

---

[10] Page 57, Open Banking Report,

"Once the customer consent is withdrawn or expires, a customer would reasonably expect that their banking data would be deleted or destroyed in order to protect their privacy"

[11] Recital 26 of the EU General Data Protection Directive excludes anonymized data from EU data protection law.

[12] Article 6(4)(e), Recital 78 and Article 25

However, Recital 26 limits the ability of data holders benefiting from pseudonymised data if re-identification techniques are "*reasonably likely* to be used, such as singling out, either by the controller or by the person to identify the natural person directly or indirectly." In other words, if de-identified aggregate data is reasonably likely to be re-identified, it cannot be used by the data holder.

We would note though that de-identified data is becoming easier and easier to re-identify. For example, privacy experts Dr Chris Culnane, A/Prof Benjamin Rubinstein and Dr Vanessa Teague of The University of Melbourne recently made a submission to the Senate Inquiry into the My Health Record System[13] that detailed the ease of re-identifying de-identified data:

> *Our research team identified both suppliers and patients in the Department of Health's de-identified MBS and PBS dataset, which was published openly online in 2016. The dataset included very little demographic information about patients, only their year of birth, state and gender. As such, a naive calculation of the "risk of re-identification" must have suggested that the risk was very low. Unfortunately, like numerous other studies in data re-identification, we could show that individuals are identifiable based on the data available: a few points of information about dates of childbirth or (other) surgeries are sufficient to identify many patients. Such demonstrations are a simple matter of knowing very few facts about the person (for example, retrieved from online news stories) and running straightforward database queries to find how many patients in the sample match.*
>
> *We do not understand the OAIC's conclusion that patients were not "reasonably identifiable" by law because of the technical difficulty of re-identification, the absence of complete confidence in all cases, and the fact that only patients with "unique or rare attributes" can be identified. The technical difficulty of finding patients is within the reach of a competent high school student. Re-identification can be made with high confidence (especially for patients with multiple data points or rare conditions) in many cases. Almost all individuals have unique linkable attributes if enough information about them is known.*

We therefore recommend that in the first instance, once an accredited CDR data recipient has provided the service as agreed in a consumer's consent or where the accredited data recipient's accreditation is revoked then the data or redundant data must be automatically destroyed.

If de-identification in some form will be allowed then genuine consent must be provided and strict EU GPDR style definitions of de-identified/anonymous data should be implemented to ensure that the data recipient is held liable when there is re-identification.

Recommendation

10. Once an accredited CDR data recipient has provided the service as agreed in a consumer's consent or where the accredited data recipient's accreditation is revoked then the data or redundant data must be automatically destroyed.

[13] f https://t.co/hsyo6072T1

11. **If de-identification in some form will be allowed then genuine consent must be provided and strict EU GPDR style definitions of de-identified/anonymous data should be implemented to ensure that the data recipient is held liable when there is re-identification**

The ACCC proposes to makes rules that will require accredited data recipients to have a system in place which allows consumers to manage their consents easily.

Financial Rights supports this proposal.

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. The ACCC welcomes stakeholder views on this proposal.

Financial Rights strongly supports the ACCC's position with respect to a prohibition on direct marketing.

One of our key concerns with the CDR regime and open Banking is the potential increase in predatory marketing practices, particularly with respect to financially vulnerable people.

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.

We will be surprised if the FinTech sector does not oppose the prohibition of the on-selling of data and use of CDR data for direct marketing. We believe that many business models will based in part or in whole on such practices. However we would urge the ACCC to not relent to inevitable pressure on this point for this first iteration of the rules or further iterations in the future.

We note that there have been some discussions at consultations on the CDR Rules that such a prohibition should not prevent particular uses that are by their nature inherent marketing such as offers for new credit cards that are central to the use of an app that seeks out better offers.

Where the marketing is inherent to the primary purpose then we would accept that this is central to the use case of the app but there should be limits on such marketing. That is simply because the offer is being sought should not allow spamming, harassment or other pressure sales tactics. Such marketing and sales tactics should also be prohibited for marketing arising as a primary purpose.

Direct marketing that arises as a secondary purpose should be prohibited outright.

With respect to the on-sale of data – this should be outright banned as we cannot see a use case or primary purpose where this would be legitimate.

Finally, Financial Rights wishes to raise an issue related to the on-sale of data; that is, the combination of CDR data with other data held by an accredited CDR participant. Credit Reporting Bureaus providing credit worthiness services or credit reports may wish to use the CDR data in combination with data already held and directly marketing credit scoring derived from the combination of this data.

Rather than strictly on-selling the data externally, in a sense the data participant would be on-selling or providing this data to another part of the business to directly market. We hope that there will be rules in place to prevent accredited CDR participants from using CDR data in combination with other datasets outset of express consents to do so and outside of any time limits to that consent. However we do think that the ACCC need to think through the scenario described here in order to prevent any direct marketing and potential exploitation of consumers through the use of CDR in other sections of the business.

Recommendation

12. **Any "marketing" or sale deemed to be central to the primary use case of a CDR participant product or service, should be subject to rules prohibiting spamming, harassment or any other pressure sales tactics.**
13. **All other direct marketing must be prohibited.**
14. **The on-sale of data should be prohibited.**
15. **Accredited CDR participants must be prevented from direct marketing other products or services arising from the use or misuse of CDR data combined with other data already or held or subsequently obtained.**

Authorisation and authentication process

Financial Rights wishes to reiterate that friction in the authorization and authentication process – ie minor impediments slowing the process such as multiple screens – is not a bad thing.

Yes, consumers seek convenience and speed over security and suitable products, however there are many cases where they do so to their own detriment. Some friction needs to be embedded into the Open Banking environment to enable better consumer decision making, particularly for harmful products.

When it comes to balancing friction with convenience, consumer safety and protection must always trump the desire for companies to produce a smooth consumer experience – a position that is based on a desire for the FinTech to net a sale rather than any real concern for consumer experience. Smooth consumer experience in this sense is a smokescreen argument for faster sales.

Financial Rights also strongly supports the creation of a *centralised* consumer dashboard to allow consumers to access and manage their authorisations easily. What we mean by centralised is one that avoids multiple consumer dashboards with each and every FinTech in each and every CDR designated sector providing their own different consumer dashboard.

Recommendation

16. A centralised consumer dashboard should be created to allow consumers to access and manage their authorisations easily across FinTech applications and across designated CDR sectors.

Providing consumer data to consumers

The ACCC proposes to make rules that require data holders to:

- **provide consumers with the ability to make requests for direct disclosure of their CDR data in a manner that is timely, efficient and convenient.**
- **allow consumers to nominate specific CDR data as part of their request, consistent with the data standards that will specify the product descriptions and information taxonomy.**
- **disclose the requested CDR data to the consumer in a variety of electronic formats, as provided for by the Data Standards Body, potentially at the election of the consumer.**

Financial Rights supports these proposals.

Use of data

The ACCC proposes to make a rule requiring accredited data recipients to identify to a consumer the uses to which the consumer's CDR data can be put, and obtain express consent to specific uses according to the consumer's wishes.

The ACCC proposes to make a rule requiring that CDR data can only be used in accordance with the consumer's express wishes, as governed by the consent process.

Financial Rights supports these proposals.

The ACCC proposes to make rules requiring accredited data recipients to transfer data to a non- accredited entity if directed by a consumer and with their specific express consent, after notifying the consumer that the entity is not accredited and disclosure is outside the protections of the CDR system.

Financial Rights remains concerned with the proposal to allow non-accredited entities to access CDR data. We believe that the ACCC must re-think its proposal. Financial Rights outlines our concerns above (in the Accreditation section) and puts forward a simple solution: that is, introduce a form of lower accreditation for entities who are not expected to be data recipients in the sense originally conceived under the Open Banking Report – ie not a FinTech, but an entity who may be acting on behalf of a consumer in a representative capacity or interacting with a consumer in some form where access to CDR data is desired or required. In other words – a form of lower tier accreditation for those conceived of under scenario 12.1.1.

In this way consumers will be provided with the necessary privacy and security protections required for handling CDR data.

In the absence of any move by the government to review the *Privacy Act* and the APPs to provide strengthened privacy protections for consumers in a modern 21st century data driven economy – the creation of lower forms of accreditation for those entities conceived of under scenario 12.1.1 will be the only way to protect consumers and ultimately maintain trust and confidence in the CDR regime as currently conceived.

We do also want to bring another issue that is likely to arise. We expect vulnerable consumer will be faced with the following scenario:

- a non-accredited provider will ask a consumer to access their own CDR data
- the non-accredited provider will request the consumer hand over that CDR data to gain the service or product on offer.

In these scenarios none of the restrictions apply re: marketing or any privacy protections and security measures.

This is slightly different from the scenarios described above, as we expect that there will non-accredited entities who will be looking to fall within the regulatory cracks and loopholes of any

accreditation system, tiered or un-tiered. For example, , new forms of debt management firms that do meet current definitions or potential tiered accreditation categories. Alternatively there will be operators who simply will not want to become accredited due to regulatory burdens.

Under the rules these dodgy operators will be able to access it via the consumer, with little redress or access to justice when things go wrong. The counter argument will be that consumers should be empowered to provide their data to anyone they wish. However it is here where consumers will be the most vulnerable to pressure tactics and unethical sales approaches to pass on their information out of the CDR system. We have already witnessed a number of shocking examples of this during the Royal Commission into the Financial Services Sector.

Such pressure or exploitation needs to be captured and prohibited by the legislation and/or rules in some form.

Recommendation

17. **The Rules or Legislation must prohibit pressure tactics being applied to consumers to hand over CDR data outside of the protections of the CDR regime.**

The ACCC proposes to make rules which would allow an accredited data recipient to disclose data to an outsourced service provider, provided the outsourcing arrangement is disclosed to consumers during the consent process and other obligations relating to outsourcing are complied with. The ACCC is also considering other rules in relation to this scenario to limit the increased risk to consumers' data, and welcomes stakeholder views on this issue.

Financial Rights supports the approach being taken here.

The ACCC welcomes stakeholder comment on a model based on use of an intermediary, to assist in determining to what extent the utility of the CDR would be limited without the ability to operate in this way.

As we understand it, an intermediary as proposed by ACCC would be an entity receiving data from the data holder and passing it on to an accredited data recipient. It is however unclear to us who an intermediary is in practice and thus cannot comment. We would request that the ACCC provide practical examples of the scenarios that they have in mind in order to better explain this concept.

Rules in relation to privacy safeguards

The ACCC also proposes:

- **in relation to privacy safeguard 1, to make rules to the effect that the CDR participant must make the policy about its management of CDR data available via its website and mobile app, in a readily accessible location and provide a copy of the policy to consumers electronically or in hard copy if requested.**

While Financial Rights generally supports the proposals put forward with respect to Privacy Safeguard 1 we believe that the ACCC needs to go further and require the following:

- *Confirmation of where the CDR participant is processing their personal data.* This means explicitly stating where a consumer's CDR will be *held* – not just in the case where the information is disclosed to a overseas accredited or non accredited entity. Information held in certain countries, such as the US will automatically allow another countries access to that data. It is important that information about international storage is provided explicitly to a consumer in order to choose whether they wish to have that information stored overseas.
- *A list of recipients (or a least the categories of recipients) with whom the data will be shared or disclosed.*
- *The period for which the data will be stored (or the criteria used to determine that period).* Given it is foreseen that there will be rules including time limits - it is essential that this be embedded in the privacy safeguards
- *Information about the existence of the rights to correction and other privacy rights including a right to deletion, a rights to restrict of processing and to object to processing as proposed by Financial Rights.* It is critical that for the sake of transparency that consumers are provided with transparent information on their rights in the privacy policy.
- *Information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the consumer.* This is critical for consumers to know how their data will be treated in an era of algorithmic bias and potential discrimination.

Recommendations

18. Privacy Safeguard 1 should be strengthened to include:

a) **confirmation of where the CDR participant is processing their personal data.**

b) **a list of recipients (or a least the categories of recipients) with whom the data may be shared or disclosed.**

c) the period for which the data will be stored (or the criteria used to determine that period)

d) information about the existence of the rights to correction and other privacy rights including a right to deletion, a rights to restrict of processing and to object to processing as proposed by Financial Rights.

e) information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the consumer.

- **in relation to privacy safeguard 2, to make rules to the effect that the use of a pseudonym by a consumer is prohibited for Open Banking.**

While we can understand the motivation behind this perspective there are some uses in open banking where a pseudonym may be appropriate.

For example, searching for better deal on a credit card, mortgage or any other credit product can impact upon your credit report. There is the possibility of multiple applications or enquires at the same time can and will impact upon a credit report. It is important that this be considered otherwise people will not wish to use particular functionality of switching services for fear of impacting upon their credit history or score.

Recommendation

19. The rules should consider the right to anonymity and pseudonymity in the open banking context for certain uses.

- **Safeguard 4: Dealing with unsolicited CDR data**

It is critical that non-accredited entities that receive unsolicited CDR data destroy this information as soon as practicable. The fact that the same requirement does not apply to non-accredited entities is a major flaw in the privacy protections applying to CDR data and should be amended.

We agree that as "soon as practicable" needs to be further defined under the rules and must veer towards immediately rather than at a time that suits.

Recommendation

20. "Non-accredited entities" as conceived under the current draft CDR legislation who receive unsolicited CDR data should be forced destroy this information as soon as practicable.

- **Safeguard 8: Cross-border disclosure of CDR data**

Financial Rights agrees that consent must be sought and received by a data participant before sending a customer's banking data overseas.

We believe that there should be an obligation on a CDR data participant to take steps to ensure that the overseas recipient does not breach the APPs in relation to CDR data.

Outside of leaking CDR out of the regime to non-accredited parties in Australia, sending data overseas will be the biggest and most obvious chink in the safety and security regime in handling personal data collection. If any breaches were to occur in an overseas jurisdiction it may be more difficult to access justice for somebody in Australia, particularly if that data is being on-sold to a fourth party based solely in another jurisdiction.

As with direct marketing, the refusal of consent should not be used to punish or penalize a customer, nor should it be used to refuse service to a customer. It should not be presented in such a way also that skews the consumer in favour of consenting.

Recommendation

21. **CDR data participants should be obliged to take steps to ensure that overseas recipient do not breach the APPs in relation to CDR data.**

22. **Consent must be sought and received by a data participant before sending a customer's banking data oversea for storage, collection or use.**

- **Privacy Safeguard 11 – Security of CDR data**

Financial Rights expresses its views with respect to de-identification above (under the Data Sets section).

- **in relation to privacy safeguard 13, to make rules to the effect that the steps the relevant persons should take should be in accordance with the steps outlined by the OAIC in relation to APP 13.**

Financial Rights can attest to a general ongoing failure to amend or correct personal information in a speedy or good faith manner. Seeking amendments to credit reports, as an example, is frustrating and difficult. Seeking corrections is important as inaccurate information can lead to say, losses under the CDR regime, notices being sent to incorrect addresses and the consequent losses that arise from that. The difficulties in seeking amendments have led to a boom in unregulated and predatory 'credit repair' businesses

This becomes even more problematic under a liability regime where a data participant will *not* be held liable for not making the changes to inaccurate, incomplete or misleading information, and merely be responsible for correcting the data (presumably in a reasonable time).

It is critical that ACCC implement rules with respect to Privacy Safeguard 12 to ensure that a CDR participant must take immediate steps to correct information once it becomes aware (by learning itself or being told by the consumer) that personal information they hold is inaccurate, out of date incomplete, irrelevant or misleading. If they do not they should be held liable for any reliance on this information that leads to a loss.

Similar to Privacy Safeguard 5 the reasonable steps standard under the current APP 12 is in no way appropriate for the CDR regime. While the draft CDR legislation states that a person "must respond to the request" rather than "reasonable steps", the steps are again those specified "in the consumer data rules" which could very well fall back on to "reasonable steps" as a standard.

We cannot support a reasonable steps standard. This standard must be modernised and CDR participants must be *required* to correct as soon as practicable.

Recommendations

23. **CDR participants must take immediate steps to correct information once it becomes aware (by learning itself or being told by the consumer) that personal information they hold is inaccurate, out of date incomplete, irrelevant or misleading. If they do not they should be held liable for any reliance on this information that leads to a loss.**

Reporting and record keeping

The ACCC proposes to make rules requiring CDR participants to keep and maintain records relating to the participant's compliance with the privacy safeguards, the rules and the standards for a period of six years.

The ACCC also proposes to make rules requiring CDR participants to keep and maintain information about complaints for a period of six years and to provide regular reports of this information to the ACCC and the OAIC.

The ACCC also proposes to makes rules requiring accredited data recipients to notify the Data Recipient Accreditor of material changes in circumstances relevant to their accreditation.

Financial Rights generally supports the proposal with respect to record keeping.

We wish to raise two issues.

Greater data gathering and monitoring powers and the use of RegTech

First, Financial Rights is keen to ensure that the ACCC, ASIC and OAIC are empowered under the CDR rules to monitor and gather data from all CDR participants in the CDR to better regulate the designated CDR sectors.

An economy based upon the use of data will have significant impacts upon consumers. We have raised these issues a number of times: algorithmic bias and discrimination; risk regimentation; price discrimination; profiling for profit; cybercrime identify theft and material theft.[14]

It is therefore critically important that all the regulators – the ACCC, OAIC and ASIC – are resourced to harness the FinTech revolution for themselves through the use regulatory technology (or RegTech) that provide the tools needed to monitor and regulate CDR participants appropriately.

For example, the ASIC or ACCC should monitor CDR participants and their use of algorithms and other black box technologies. RegTech could be used to access these commercially sensitive programs to identify price discrimination, algorithmic bias and discriminatory practices. Access to CDR product information by regulators could also assist in competition, pricing and product strategies to ensure they are meeting the law.

ACCC, OAIC and ASIC should also gather broader data using RegTech to develop regular market analyses to examine actual consumer outcomes in the CDR space. The information gathered could also be used to provide information to empower consumers and promote competitive markets.

The information and data gathered via RegTech could also assist evaluating the CDR program.

The CDR Rules being developed should therefore reflect a broader data collection remit to more closely monitor the sector.

With the Banking Royal Commission we have already witnessed what occurs when there is limited monitoring of the day to day running of profit hungry financial services businesses.

It is time for regulators to be more proactive in their monitoring otherwise it is likely we will be requiring a Royal Commission into the CDR sector in 5 to 10 years. The introduction of Product Intervention Powers and Design and Distribution Obligations should mark the beginning of a preventative regulatory philosophy rather than curative approach. The approach of responding and addressing problems after the fact should be consigned to the dustbin of history.

Consent and authorisation recordkeeping and access by consumers and their representatives

The second issue that has yet to be considered is consent record keeping and access to consents and their records by consumers and their representatives.

---

[14] For further information on this see Financial Rights Submission to the Australian Human Rights Commission re: Human Rights and Technology Issues Paper, October 2018 http://financialrights.org.au/wp-content/uploads/2018/10/181002_HRTechIssuesPaper_Submission_FINAL.pdf

It is highly likely that Financial Rights and other legal centres will receive complaints from consumers with respect to the abuse, misuse or breach of CDR data by a FinTech. One issue that may be in dispute will be what did the consumer consent to in using the service or product and whether consent was genuine and freely given. In order to assess this, or for a consumer to examine this and complain themselves, consumers and legal representatives will need to be able to access these electronic consents.

ACCC needs to implement rules to ensure that not only will there be an accessible consent and authorisation dashboard page that maintains their authorisations but consumers and their representatives need to have access to the original consents pages and processes in order to examine whether a consent was genuine and freely given. Historic authorisations will be maintained according to the proposals under 9.8 but will the process of gaining that authorisation be captured?

Consumer will need to be able to assert their rights post consent and authorisation. If there is some confusion over the consent provided – say the consumer misunderstood what they were consenting to or the wording was in fact ambiguous – consumers and their representatives need access to the original consents in order to assess the consent.

Is it the case that the ACCC will be checking each and every consent page to ensure that it meets the standards of consent required? We presume not. Representatives of the ACCC suggested that this would not be the case at the recent consultations.

We are also aware of the circumstance with some FinTechs in the Buy Now Pay Later space where a consumer who has defaulted on a payment have been locked out of their online account or App. This means that they are unable to access basic information about the account including at least in this case: balance outstanding, fees accruing etc.

Financial Rights can see that the same scenario may arise during a dispute with a Data Participant. That consumer should be able to have access to all relevant and appropriate information including consents.

Recommendations

24. **ACCC must establish record keeping and monitoring rules with respect to the use of algorithms and other black box technologies**

25. **Regulators including ACCC, OAIC and ASIC must be empowered to gather more data and monitor CDR participants via RegTech to develop regular market analyses to examine actual consumer outcomes in the CDR space and evaluate the success or otherwise of the CDR regime.**

26. **Rules must be established regarding the recording of the original consent and authorisations in order for consumers and their representatives to access in the event of a problem and complaint and consent is material to the matter.**

27. **CDR consumers should never be locked out of accessing their own information with a data recipient and reasonable access should be provided online and/or via the FinTech app or centralised consumer dashboard.**

Dispute resolution

In relation to internal dispute resolution, the ACCC proposes to make a rule requiring that all CDR participants have in place internal dispute resolution procedures that comply with the requirements specified in the rules.

Financial Rights supports this proposal.

In relation to external dispute resolution, the ACCC proposes to make a rule requiring that all CDR participants be a member of the external dispute resolution scheme recognised by the ACCC for Open Banking. The ACCC proposes to recognise the Australian Financial Complaints Authority (AFCA).

Financial Rights supports this proposal.

Concluding Remarks

Thank you again for the opportunity to comment. If you have any questions or concerns regarding this submission please do not hesitate to contact Financial Rights on (02) 9212 4216.

Kind Regards,

Karen Cox
Coordinator
Financial Rights Legal Centre
[redacted]