Submission by the Financial Rights Legal Centre and Financial Counselling Australia

Treasury

Treasury Laws Amendment (Consumer Data Right) Bill 2018

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

About Financial Counselling Australia

Financial Counselling Australia is the peak body for financial counsellors. Financial counsellors assist people experiencing financial difficulty by providing information, support and advocacy. Working in not-for-profit community organisations, financial counselling services are free, independent and confidential.

Introduction and Executive Summary

Thank you for the opportunity to comment on the *Treasury Laws Amendment (Consumer Data Right) Bill 2018*. The Financial Rights Legal Centre (**Financial Rights**) has drafted this submission Financial Counselling Australia, the peak body for financial counsellors in Australia, has endorsed this submission and concurs with the concerns raised.

Financial Rights has made a series of submissions to the Productivity Commission's Data Availability and Use and Open Banking Review.[1]. These submissions outline a series of fundamental concerns that we had hoped would be addressed in the development of an open banking and consumer data right regime. In summary these concerns are:

- **Increased complexity and choice:** Greater choice, increased competition and new products may bring some benefits to some people, however greater complexity, choice and transaction speeds in open banking and consumer data products and services will likely result in information overload and too little time to make decisions, less consumer understanding and market inefficiencies.
- **Increased economic inequality and financial exclusion:** Risk segmentation, profiling for profit, price discrimination and the delivery of poor, unsuitable products are all likely outcomes of greater access to consumer data. Those experiencing financial hardship are often very profitable to companies and therefore most vulnerable to exploitation. Those in more precarious financial situations are more likely to be unfairly charged higher amounts or pushed to second tier and high cost fringe lenders.
- **Increased information asymmetry and predatory marketing:** Access to data and continuous monitoring are likely to lead to predatory practices, for example by payday lenders. There is also an increasing asymmetry of power in consent provision and contracting.
- **Increased unconscionable practices:** Closed proprietary algorithms could potentially lead to situations where consumers are denied access to crucial products and services based on inaccurate data without the ability to determine why or to correct underlying assumptions**.** Increased use of non-transparent, black box technology could also lead to

[1] Joint consumer submission on the Open Banking: customers, choice, convenience, confidence Final Report, March 2018 http://financialrights.org.au/wp-content/uploads/2018/03/180323_OpenBanking_FinalReport_Sub_FINAL.pdf; Joint supplementary submission by the Financial Rights Legal Centre and Consumer Action Legal Centre Treasury Open Banking: customers, choice, convenience, confidence, December 2017 http://financialrights.org.au/wp-content/uploads/2017/10/171025-Open-Banking-Supplementary-Submission-FINAL.pdf, Joint submission by the Financial Rights Legal Centre and Consumer Action Legal Centre Treasury Open Banking: customers, choice, convenience, confidence, October 2017, http://financialrights.org.au/wp-content/uploads/2017/09/170922-FINAL-submission-open-banking-issues-paper.pdf; Submission by the Financial Rights Legal Centre Productivity Commission Draft Report: Data Availability and Use, October 2016 http://financialrights.org.au/wp-content/uploads/2016/12/161216_FRLCSubmission_draft-report-Data-Availability-use.pdf

poor consumer outcomes through the creation of potentially biased and discriminatory algorithms.

- **The use of inaccurate or flawed data with few avenues for individuals to correct errors in an efficient and prompt manner.**
- **Increased privacy concerns relating to the security, portability and use of financial and personal data.**

Financial Rights notes that the current Consumer Data Right (**CDR**) legislation addresses very few of these concerns and those concerns that is does seek to deal with, it fails to address in any comprehensive manner.

Consequently, Financial Rights believes that the draft CDR legislation (and approach) is misconceived and fundamentally flawed in a significant number of ways.

The CDR is limited in scope and misleads consumers

The "Consumer Data Right" has been named and presented in a way that seems like it is establishing an all-encompassing, comprehensive consumer right. It is not. The "Consumer Data Right" is a misnomer. It is a Consumer Data *Portability* Right. It is not the introduction of a comprehensive set of consumer data rights like the European Union's General Data Protection Right (**GDPR**)**.** This is implicitly acknowledged in the *Exposure Draft Explanatory Materials.*[2]

The CDR is merely a collection of rights with respect to porting or transferring consumer data. It provides no further rights to more broadly access your data, restrict processing, object, delete, correct, rectify one's data. The CDR is therefore misleading as consumers are being sold the idea of a "consumer data right" to protect consumers in their access to and use of their own financial data. Once outside of the system, lower or non-existent privacy rights apply.

The CDR is piecemeal and expedites Australia falling behind the rest of the world

The portability rights created by the CDR will only apply to designated sectors as approved by the Minister. Currently this will be applied to the banking sector but will expand to cover other sectors such as energy, telecommunications, insurance, even social media. Given the timelines proposed, the application of strengthened privacy standards will take decades to spread to all aspects of the economy.[3]

Compare this to the approach being taken by the EU. The new EU GDPR has established a list of 20 Data Protection Rights that applies to all individuals and businesses across the entire economy including the Right to Access, Right to Deletion, Right to Rectification, etc. One of those rights is the Right to Portability. In this sense this "Consumer Data Right" will be one twentieth of the rights being provided to EU citizens, leaving Australian industry and consumers well behind.

---

[2] Para 1.1 "*The Consumer Data Right (CDR) will provide individuals and businesses with a right to efficiently and conveniently access specified data in relation to them held by businesses; and to authorise secure access to this data by trusted and accredited third parties."*

[3] The EDEM only states that: "*Over time it is expected that these same benefits will be rolled out to other sectors of the economy.*[3]

Australian FinTechs wishing to work and compete internationally will have to establish multiple privacy safeguards and systems, placing our businesses at a strategic disadvantage.

The CDR establishes multiple privacy standards, confusing consumers and placing them at risk

The CDR creates a third privacy standard that applies to consumers seeking protection, security and redress when something goes wrong with their data. The CDR Data Privacy Safeguards as envisioned under this draft legislation will be an addition to the current Australian *Privacy Act* safeguards as detailed under the Australian Privacy Principles (**APPs**). Then there are the general consumer protections and laws that apply to those situations where holders of consumer data are *not* "APP entities" as defined under the APPs[4].

The introduction of the CDR is an explicit acknowledgement that the current APPs are out of date, no longer fit for purpose, and are generally weaker than what is required for a modern data-based economy, ie the APPs are not good enough to provide the privacy protections that consumers require.[5]

Implementing the CDR alongside the APPs implements multiple privacy standards. This will be confusing for consumers and industry alike. It also leaves consumers vulnerable to lower protections in different situations given the ability for non-accredited parties to gain access to CDR data.

The CDR facilitates the leakage of sensitive financial data to entities that provide lower privacy protections

The aim of the CDR is to create a safe and secure environment in which consumers will be able to trust and have confidence that they will be able to transfer or port their data from one data holder or participant to another.

However the CDR facilitates non-accredited parties obtaining CDR information, leaving these consumers, who were led into a system on the promise of higher privacy protections, vulnerable to the lower privacy standards of the APPs. This is a fundamental flaw to the legislation and needs to be reconsidered.

The CDR establishes flawed and incomplete privacy safeguards

Even when a consumer is subject to the CDR privacy safeguards which match to the APPs, the stronger safeguards are limited and incomplete. They:

- do not provide a right to deletion or erasure
- do not embed privacy by design
- do not provide the right to restrict purposes
- do not provide the right to object to processing; and
- do not provide the right to not be evaluated on the basis of automated processing.

[4] ie all private sector and not-for-profit organisations with an annual turnover of less than $3 million

[5] Pages 54-56, Recommendation 4.2 – modifications to privacy protections.

The CDR institutes two very different FinTech sectors

In addition to the multiple privacy standards, the CDR embeds two very different FinTech sectors by not banning screen scraping and other unsafe technologies. These unsafe data access technologies have been banned in other countries. Providing access to this 'screen scraping' technology can amount to a breach of the terms and conditions of a customer's bank account, and can put customers at risk of losing their protections under the E-Payments Code[6] This will impact harshly upon financially vulnerable consumers. Without a ban on these technologies, there is very little incentive for businesses such as pay day lenders and debt management firms to become accredited. The higher regulatory hurdles will in fact be a disincentive to these businesses from joining. Financially vulnerable people, for example, will continue to be desperate to access credit and will not concern themselves with the nuances of privacy protections to so. If that means engaging with non-CDR accredited entities like pay day loan operators, those financially vulnerable people will end up with lower privacy protections than their middle-class counterparts.

Key Recommendations

Given the above, Financial Rights recommends a complete re-think in the approach Treasury has taken with respect to the implementation of the CDR.

1. The CDR legislation should not be finalised nor implemented until the *Privacy Act* and the Australian Privacy Principles are reviewed and strengthened to reflect the needs of a modern economy based on access to and use of consumer data.
2. If the Government insists on proceeding with the current draft CDR legislation and approach then a number of significant changes need to be implemented.
3. The CDR legislation needs to be re-named to the Consumer Data Portability/Transfer Right to reflect the actuality and intent of its operation.
4. As clearly recommended by the Open Banking Review, the CDR legislation should be a closed system to prevent any CDR data being provided to any non-accredited entity. 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 can be appropriate to their use and be implemented on a sliding scale if need be.
5. The CDR legislation must ban all screen-scraping and other unsafe data access, transfer and handling technologies as has occurred in the UK and elsewhere.
6. The CDR must implement stronger privacy safeguards to those currently proposed and introduce further safeguards and security measures currently not conceived of under

[6] See discussion in the Final Report of the Small Amount Credit Contract Review, March 2016, at p. 76-77, available at https://static.treasury.gov.au/uploads/sites/1/2017/06/C2016-016_SACC-Final-Report.pdf.

the APPs but which are necessary for a modern, forward looking, consumer data transfer regime that will build genuine consumer trust and confidence.

Response to the Treasury Laws Amendment (Consumer Data Right) Bill 2018 Proposals

Designated sectors

By design, the draft CDR legislation will apply to different sectors of the economy that have been designated by the Minister.

Under the CDR regime, individuals and businesses can directly access or direct that their data be shared with certain CDR participants and seemingly non participants under certain circumstances.

The development of this legislation and the CDR model more broadly emerges from the government's response to both the Productivity Commission's Inquiry into Data Availability and Use Report and the Review into Open Banking in Australia 2017 which recommended that Open Banking be implemented through a broader CDR framework.

While this approach may be appropriate to developing consistent application programming interfaces (**APIs**) and data standards for vastly different sectors of the economy and their unique data sets (banking and financial information versus energy, telecommunications, social media, insurance and other sectors yet to be identified), it fails to 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 EU who has established a list of 20 Data Protection Rights that applies to all individuals and businesses across the entire economy including the Right to Access, Right to Deletion, Right to Rectification, etc. The EU has established this baseline set of safeguards and is also systematically developing rules and data standards for every sector to more appropriately implement consumer facing data products and services such as open banking.

The draft CDR legislation however only implements one of the rights that the EU has implemented - the right to portability. In this sense then the CDR is a misnomer as it is merely a Consumer Data Portability/Transfer Right.

While this is implicitly acknowledged in the *Exposure Draft Explanatory Materials*[7] the Government is selling the CDR in such a way that suggests that the CDR is a broader right:

> *This Bill is a game changer for Australians. The Consumer Data Right will empower customers to use their data for their own benefit. … Customers will determine which data is shared, on what terms and with whom. The Consumer Data Right is a right for customers and not for those who wish to access or use a customer's data. …The Government is committed to ensuring that high levels of privacy protection and information security for customer data is embedded in the new regulatory framework. This Bill delivers enhanced protections, backed by well-resourced regulators with strong powers.* [8]

Counter to the sales pitch, the CDR is merely a collection of rights with respect to porting or transferring consumer data in certain designated sectors. It provides no further rights to more broadly access your data, restrict processing, object, delete, correct, or rectify your data. The CDR is therefore misleading as consumers are being sold the idea of a "consumer data right" to protect consumers in their access to and use of their own financial data.

All that is being created is a set of standards to be applied to the portability of consumer data with some strengthened privacy safeguards in specific designated sectors.

While these strengthened privacy safeguards are welcome, the CDR is in essence establishing a third set of privacy standards for specific designated sectors that applies to consumers seeking protection, security and redress when something goes wrong with their data.

The CDR Data Privacy Safeguards as envisioned under this draft legislation for specific designated sectors will be an addition to the current Australian *Privacy Act* safeguards as detailed under the Australian Privacy Principles (**APPs**).

The APPs are also in addition to general consumer protections and law that apply to those situations where holders of consumer data are *not* "APP entities" as defined under the APPs[9].

The introduction of the CDR for designated sectors are an explicit acknowledgement that the current APPs are out of date, no longer fit for purpose, and are generally weaker than required for a modern data based economy, ie the APPs are not good enough to provide the privacy protections that consumers require.[10] The Open Banking Report details an extensive list of modifications that will be required to boost the protections required for a modern open banking system. This includes:

- APP3 not requiring informed and express consent;

---

[7] Para 1.1 "*The Consumer Data Right (CDR) will provide individuals and businesses with a right to efficiently and conveniently access specified data in relation to them held by businesses; and to authorise secure access to this data by trusted and accredited third parties.*"

[8] The Hon. Scott Morrison, Treasurer, Media Release *More power in the hands of consumers*, 21 September 2018, http://sjm.ministers.treasury.gov.au/media-release/087-2018/

[9] ie all private sector and not-for-profit organisations with an annual turnover of less than $3 million

[10] Pages 54-56, Recommendation 4.2 – modifications to privacy protections.

- APP 5 merely requiring reasonable steps be taken to notify consumers rather than having to notify; and
- APP 7 not requiring express and informed consent for direct marketing.

The Open Banking Report lists six changes that would be required.

Implementing the CDR alongside the APPs therefore implements multiple privacy standards. This will be confusing for consumers and industry alike. This is especially the case given the fact that as envisioned under the Act, sensitive personal financial data will be subject to these different standards in different circumstances and different stages of the data lifecycle: this is explained further below regarding financial data under the non-accredited data recipients section, below.

Financial Rights therefore believes that while designate sectors to establish and introduce data standards for the purposes of portability, is sensible the approach being taken by the Treasury to designate sectors for increased privacy protections needs to be reconsidered.

Financial Rights recommends that the CDR legislation should not be finalised nor implemented until the *Privacy Act* and the APPs are reviewed and strengthened to reflect the needs of a modern economy based on access to and use of consumer data. In addition to the problems identified by the Open Banking review which demonstrate how the APPs are inappropriate for a modern, data based economy, there are other issues with the APPs. The last time privacy laws in Australia were comprehensively reviewed was ten years ago.[11] The way Australian consumers and businesses use and supply data has changed dramatically since then. Australians' expectations for privacy have also increased markedly, in line with increased awareness of the importance of personal data and increased breaches in their personal data. Add to this, significant international developments in privacy protections and the APPs stand as a relic of a former time and are in no way fit to address community expectations with respect to the use, security and protection of their data.

If the Government insists on proceeding with the current draft CDR legislation and approach then a number of significant changes to the current draft need to be implemented.

The CDR legislation needs to be re-named to the Consumer Data Portability/Transfer Right to reflect the actuality and intent of its operation. Without this change consumers will continue to be misled about the scope and reach of the CDR and may fall into a false sense of security.

As clearly recommended by the Open Banking Review, the CDR legislation should be a closed system to prevent any CDR data being provided to any non-accredited entity. 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 can be appropriate to their use and be implemented on a sliding scale if need be. See further information on this under the Participants in the CDR System, below.

[11] ALRC, *For Your Information: Australian Privacy Law and Practice*, Report 108 , 12 August 2008. Available at: https://www.alrc.gov.au/publications/report-108

Recommendations

1. **The CDR legislation should not be finalised nor implemented until the *Privacy Act* and the Australian Privacy Principles are reviewed and strengthened to reflect the needs of a modern economy based on access to and use of consumer data.**
2. **If the Government insists on proceeding with the current draft CDR legislation and approach then a number of significant changes need to be implemented:**
   a) **The CDR legislation needs to be re-named to the Consumer Data Portability/Transfer Right to reflect the actuality and intent of its operation.**
   b) **The CDR legislation should be a closed system to prevent any CDR data being provided to any non-accredited entity.**
   c) **All handlers of CDR data should be accredited. This accreditation should be appropriate to their use and be implemented on a sliding scale if need be.**

Participants in the Consumer Data Right System

Non-accredited data recipients

The EDEM states that there will be circumstances where non-accredited entities will be able to access CDR data:

> *1.47 In certain circumstances, CDR consumers can direct that their CDR data be provided to a non-accredited entity. Data that has been derived from CDR data, such as financial reports compiled from transaction data, may also be transferred by a CDR consumer out of the CDR system. For example, to their accountant. However, the collection, storage, use and disclosure of that information will be regulated via the APPs, if applicable. **[Schedule 1, item 1, sections 56BB and 56BC)]** (our emphasis)*

This is a fundamental flaw to the CDR regime and should be reconsidered.

Access by non-accredited parties is *not* what was recommended under the Open Banking Report. The Open Banking Report explicitly recommends:

> *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.*

The reason? The Open Banking Report states that:

For customers to have confidence in Open Banking they will need assurance that other participants — data holders and recipients — are accredited entities that will adhere to appropriate security and privacy standards and have the capacity to provide financial compensation if things go wrong and they are found liable.

…Other participating entities should be required to establish that they can safely deal with their obligations in relation to data (which may not necessarily be as stringent as the prudential obligations for banks). The standard that non-ADIs may be required to meet should be based on the potential harm to customers, and risk to the Open Banking system, that the relevant data set and that participant pose. [12]

Consumer confidence in Open Banking and the CDR is crucial if it has any chance of succeeding.

The decision to allow non-accredited entities to access sensitive CDR data is incredibly dangerous. It is dangerous because consumers are being led to assume their data will be protected under a "Consumer Data Right" but in fact it is facilitating the movement of this data to lower privacy protections.

As mentioned above, the introduction of the CDR regime 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 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.

[12] Pages 44-5, Open Banking Report https://static.treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open-Banking-_For-web-1.pdf

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"[13] 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 final category of low standard privacy protections is explicitly foreseen by Treasury through the use of the words "if applicable", emphasised above, under paragraph 1.47

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 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 protection for consumers.

This is unacceptable.

Financial Rights notes the example provided Example 1.16 that demonstrates one potential scenario. It states:

> *Naomi currently banks with BankOz but she has accepted a position with a company that will see her moving to New York at the end of the year. Naomi feels that the role will be ideal for her and is interested in purchasing a property in Manhattan as her New York base but she has no history with BankUSA who she wishes to transfer all of her savings and credit accounts to once she relocates to New York.*
>
> *Naomi asks BankOz to transfer all of her personal information to BankUSA under APP 12, because BankUSA is not an accredited data recipient under the CDR.*
>
> *BankOz must comply with APP 8 in relation to the cross border disclosure of Naomi's personal information as it is not covered by the privacy safeguards, due to BankUSA not being an accredited data recipient.*
>
> *The transfer is of Naomi's personal information, rather than CDR data (even though it may be the same information), because it occurs under the Privacy Act.*

[13] 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

The first thing to note about this example is that while the *transfer* of Naomi's personal information will be subject to the *Privacy Act* and the APPs rather than the CDR privacy safeguards, the *subsequent* holding and use of that data will be subject to US laws and privacy safeguards. While there may be a case to be made for those circumstances where CDR information will need to be transferred to foreign entities, these will ultimately left to the laws of the country where the foreign entity lies.

The more important and relevant issue relates to the the circumstance of Naomi's personal information being held and used by a non-accredited entity *in Australia*. This will be a vastly more common occurrence than a transfer overseas.

If Naomi were to ask that BankOz transfer her CDR data to, say, a local sole trading accountant (as suggested at para 1.47) and that accountant is neither an accredited CDR entity nor an "APP entity" any use, misuse or breach of that data will not necessarily be subject to the protections under the CDR Privacy Safeguards nor the *Privacy Act* or APPs. Given the current definition of an APP entity and OAIC checklist, it is likely that an accountant could easily fall outside of the definition of APP entity and any of the requirements for small businesses.

Other than accountants, there are a multitude of potential entities who may seek to access CDR data as a non-accredited entity. These include:

- 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.

Non-accreditation and consent of a consumer

Even if a consumer consents to a transfer out of the CDR regime to a non-accredited entity, this could result in significant problems.

While unclear and not guaranteed, we assume that CDR rules will be developed by the ACCC in consultation with stakeholders and will be in place to ensure that consumers will be made aware that their CDR data will be provided to a non-accredited entity. We also assume, and again there is no guarantee to this, that the consumer will be told that the CDR data will no

longer be subject to the CDR Privacy Safeguards, but be subject to the Privacy Act and APPs or even not be subject to either set of protections.

This raises a number of questions/issues.

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.

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. And 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 CDR legislation.

This is particularly the case with respect to pay day lenders.

The draft CDR legislation does not ban screen scraping and other technologies. These incredibly unsafe data access technologies have been banned in other countries. Without a ban on these technologies, there is very little incentive for businesses such as pay day lenders and debt management firms to become accredited. The higher regulatory hurdles will be a disincentive to these businesses from joining. Financially vulnerable people will of course continue to be desperate to access credit and will not concern themselves with the nuances of privacy protections to so. If that means engaging with non-CDR accredited entities like pay day loan operators, financially vulnerable people will do just that.

Even non-financially vulnerable consumers may hold misplaced trust in a financial advisor or accountant that they know. Indeed there is significant research that trust increases when a financial advisor provides information on conflicts of interest because the consumer believes they are being transparent and therefore is more deserving of trust.[14]

[14] James Lacko and Janis Pappalardo, *The effect of mortgage broker compensation disclosures on consumers and competition: A controlled experiment, Federal Trade Commission Bureau of Economics Staff Report,* 2008

The principle could very well apply with respect to greater disclosure and transparency with respect to the application or lack thereof of privacy safeguards. If the scandals in financial advice, mortgage and insurance broking that led to the current Royal Commission are anything to go by, this will continue to the be the case.

It has been put to Financial Rights in CDR consultations that consumers don't need to know which set of privacy standards they will be subject to since there will be an "any door approach" to EDR and complaints handling and the appropriate EDR will figure it out. This dismisses the fact that people will be afforded fewer safeguards depending on where they happen to fall in the process.

As we read the legislation, there is nothing preventing the ACCC from developing rules of accreditation for all potential small businesses and sole traders who are currently conceived to possibly gain access to CDR data as a "non-accredited entity". In other words, the ACCC could very well introduce accredited rules and standards not simply to FinTechs to be accredited, but for all accountants, financial advisors, and mortgage brokers on a sliding scale, to ensure that consumers are protected under the CDR privacy safeguards. We do not believe that this would be in any conceivable way onerous. Accessing huge amounts of personal financial information is not a right and should be a privilege one that comes with obligations to protect the privacy of individuals and meet expected security standards. Providing people with access to huge amounts of private financial information under the CDR is *not* business as usual.

We believe that if the Treasury proceed with the legislation in its current form then the ACCC must implement accreditation rules for these data recipients.

There is also nothing preventing the legislation from being re-drafted to ensure that all CDR data, wherever and whoever it is held by, will be subject to CDR privacy safeguards. This was, in our view, the original intent of the Open Banking Report.

The reason, for example, why the UK does not have to worry about leakages outside of their own Open Banking regime is because the GPDR rules are in place for all citizens and their data across the economy. These general protections do not exist in Australia.

The simplest solution, as recommended above, would be to delay the introduction of the CDR regime until the Privacy Act and the APPs are modernised to meet community standards and requirements arising from technological development.

In the absence of any such review Financial Rights recommends that the CDR legislation should be a closed system to prevent any CDR data being provided to any non-accredited entity. 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 can be appropriate to their use and be implemented on a sliding scale if need be.

---

referenced in Financial Services Authority, Financial Capability: A Behavioural Economics Perspective, 2008

> *"Even if the disclosure is noticed by consumers, it may have the effect of increasing trust in advisers rather than making consumers more wary."*

The CDR legislation must ban all screen-scraping and other unsafe data access, transfer and handling technologies as has occurred in the UK and elsewhere.

Accreditation process

Financial Rights supports the establishment and implementation of a strong accreditation process and accreditation criteria to ensure consumer protections are built into the system from the start.

Accreditation is crucial to the success of the CDR. As the Open Banking Report stated:

> *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.*[15]

Without accreditation, trust and confidence falls away.

Financial Rights has stated emphatically that all entities seeking to use or hold CDR data must be accredited – with no exceptions.

This means that accreditation needs to be implemented for those potential financial services users who are currently conceived under the legislation to be "non-accredited," but in our strong view should be accredited. At a minimum these entities – including accountants, financial advisors, mortgage brokers, etc should afford consumers CDR privacy safeguards and protections and adhere to most if not all of the accreditation criteria we list below.

Financial Rights supports a tiered model for accrediting entities based on differing levels of risk and potential harm and we would support a system that varies the obligations as to a FinTech company, a neo-bank or a financial advisor or accountant.

But it is critical that *all* of these entities (companies and individuals) handling CDR data must be accredited.

Placing the non-accreditation issue aside, we do support the proposals to empower the ACCC as foreseen by the Open Banking Report to create the data rules as listed in the EDEM including:

- about the powers and functions of the Data Recipient Accreditor;
- about specific criteria to be applied to persons seeking to be accredited under subsection 56CE(1);

[15] Page 22, Open Banking Report https://static.treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open-Banking-_For-web-1.pdf

- outlining that accreditations may only be provided subject to applicants meeting certain conditions, including the ongoing imposition of conditions on accredited entities after accreditation has been granted;
- allowing for accreditation to be provided at different levels taking into account the different risks associated with the kind of activities undertaken within that designated sector or the kinds of applicants;
- relating to the period, renewal, transfer, variation, suspension, revocation or surrender of accreditations;
- outlining transitional rules for when an accreditation is suspended or ends and the treatment of data under such circumstances; and
- about the Register of Accredited Data Recipients.

Accreditation criteria

While it may be more appropriate to outline our views with respect to criteria that the ACCC should set for accreditation, the Treasury should be aware of our position to ensure that the legislation is compatible.

Financial Rights believes there needs to be the following baseline criteria to which all tiers must adhere. These include:

- meeting privacy standards and security standards including providing a description of the process in place to file, monitor, track and restrict access to consumer data;
- demonstrating that they have the technical capabilities to meet the standards,
- adhering to mandatory breach notifications;
- establishing risk management processes and measures including procedures to deal with security incidents;
- adhering to trust accounting rules and other measures taken for safeguarding payment service users' funds, where applicable;
- establishing Internal Dispute Resolution (**IDR**) processes;
- membership of an EDR body i.e. AFCA (as proposed);
- processes that establish genuine customer consent including testing procedures to demonstrate that customers understand what has been consented to (see further below);
- the collection of statistics/data on performance, transactions and fraud for the use of regulators;
- ensuring that all primary and secondary uses of any product or service meet a set of ethical standards or principles; and
- no history of data breach or misuse, or of disregard for the law.

The EU Payment Services Directive (**PSD2**) provides important guidance as to what should be included in accreditation criteria. Many of these requirements should be able to be met by any

potential FinTech wishing to engage in the Open Banking System. Many of them are included in our list above and are simply basic business documentation including:

- a description of the type of service being offered: EU PSD2 Article 5 (1)(a)
- a business plan including forecast budget for the first 3 years: EU PSD2 Article 5 (1)(b)
- evidence that the business holds an appropriate level of initial capital: EU PSD2 Article 5 (1)(c)
- a description of the governance arrangements of the business including control mechanisms: EU PSD2 Article 5 (1)(e)
- a description of the business continuity arrangements and contingency plans: EU PSD2 Article 5 (1)(h)
- a description of the business' structure and outsourcing arrangements: EU PSD2 Article 5 (1)(l)
- evidence of the suitability of the board's management, and directors: EU PSD2 Article 5 (1)(l)&(m)
- the identity of auditors: EU PSD2 Article 5 (1)(o)
- the applicant's legal status and article of association, and the address of the head office: EU PSD2 Article 5 (1)(p) & (q).

Protecting sensitive information

Financial Rights also notes that actually defining high risk versus low risk for the purposes of a tiered accreditation system may be difficult.

A person's financial circumstance is highly sensitive since a breach opens them up to exploitation by unscrupulous operators, price discrimination and other risks. There are many forms of personal financial data that are highly sensitive due to the serious risks of hacking (account details, passwords), material theft, and identity theft (credit card numbers, ccv numbers).

Currently "sensitive information" is defined under the *Privacy Act* to mean information or an opinion about an individual's:

- racial or ethnic origin;
- political opinions;
- membership of a political association;
- religious beliefs or affiliations;
- philosophical beliefs;
- membership of a professional or trade association;
- membership of a trade union;
- sexual preferences or practices;

- criminal record;
- health information; or
- genetic information.

Sensitive information in this context is information that could be used as the basis of unjustified discrimination. This is appropriate.

It is our view that there is a likelihood that CDR data can and likely will be used to discriminate. Sensitive financial information can and will be used to both:

- discriminate via the use of black box algorithmic biases that contain proxy variables that stand in for omitted categories such as postcode for race and ethnic origin, the purchase of certain goods or services for sexual identity, religious or political affiliation etc.; and
- price discrimination where Australia's most vulnerable, disadvantaged and financially stressed households are identified and for example unfairly charged higher amounts for credit, or be pushed to second-tier and high cost fringe lenders.

Sensitivity is therefore contextual. Certain information in the hands of one party may be mundane and uncontroversial but highly sensitive and consequential in others. The current definition of sensitive information in the *Privacy Act* does not include financial information, which is surprising and disappointing given the new ways discrimination may arise through the misuse of data analysis and black box algorithms.

It is our view that their needs to be a full reconsideration of the concept of sensitivity under the *Privacy Act* to ensure that financial data is also considered sensitive, less because of the chance of discrimination (although there is such a potential) but more because if it were to be breached, and not handled with appropriately high standards, it will lead to serious financial consequences.

Given the move to an economy based on the use of personal data in almost every aspect of life, there needs to be greater protections under the *Privacy Act* and that involves consideration of further shades of sensitivity to cover the multiplicity of problems that can arise that are incongruent with the current binary approach.

In the meantime, the current CDR legislation and CDR rules should include accreditation criteria that bans and regulates any price discrimination, algorithmic discrimination and black box algorithms inaccessible to regulators.

Problematic business models

One key concern of Financial Rights is the business model of FinTechs particularly "Freemium" models that in part will make money from advertising or the sale of data and information to "fourth parties"[16] in Australia or overseas.

Any business model dependent upon the on-sale of personal data to fourth party entities (be they CDR accredited or non CDR accredited) is one that has the potential to sell this data to any and all entities including unscrupulous or disreputable international or Australian parties who have a history of misuse of data through spamming, hacking or other activities that don't comply with the law or meet community expectations.

At minimum, the sale of this data to fourth parties needs to be regulated and overseen under the scheme via the accreditation criteria (or some other method). We would prefer the practice be banned outright.

Screen-scraping, the CDR regime and accreditation

Establishing an accreditation process without banning other unsafe forms of accessing personal financial transactions such as screen-scraping creates a multitude of issues.

By not banning screen scraping and other unsafe access technologies – as has occurred in other jurisdictions including the UK - two very distinct FinTech sectors will be created: a sector that will adhere to higher privacy safeguards and standards and a sector that will not. It is unclear what the incentives are to seek accreditation under the CDR for, say, a screen-scraping pay day lender. While there are many pay day lenders or debt management firms, for example, who may seek reputational legitimacy, many others do not. The additional hurdles, regulations, obligations introduced by an accreditation process will remain unattractive to many of these businesses, some of whom already skirt the regulations in place. With a steady stream of desperate and vulnerable clientele willing to do anything for a speedy solution or fast cash, there is no financial, reputational or other incentive for them to seek accreditation,

Financially vulnerable people *will* continue to be desperate to access credit and will not concern themselves with the nuances of privacy protections to so. If that means engaging with non-CDR accredited entities like pay day loan operators they will. The result will be financially vulnerable people will ending up with lower privacy protections than their middle-class counterparts.Screen-scraping can amount to a breach of the terms and conditions of a customer's bank account, and can put customers at risk of losing their protections under the E-Payments Code.[17]

[16] If the consumer is the first party, the bank data-holder is the second party, the data recipient is the third party, then we refer to other parties to which data is on-sold or provided to by the third party data holder as "fourth parties". This is an important distinction to make when considering the downstream uses and potential abuses of data and data breaches.

[17] See discussion in the Final Report of the Small Amount Credit Contract Review, March 2016, at p. 76-77, available at https://static.treasury.gov.au/uploads/sites/1/2017/06/C2016-016_SACC-Final-Report.pdf.

Fees

Financial Rights notes that the ACCC may also make a rule in relation to establishing a fee for accreditation and it must reflect the administration cost of the accreditation process.[18] This should also cover the costs of ongoing administration of the accreditation system not simply the initial accreditation process.

Register of accredited entities and the Accreditation Registrar

Financial Rights notes the proposal to create a register of Accredited Data Recipients and an Accreditation Registrar. This is appropriate. We wish to note our support for proposed section 56CK(4)(c) and argue that this 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.

Recommendations

3. **Financial Rights supports a tiered accreditation regime however there must be baseline accreditation criteria that all tiers must adhere including:**

    a) **meeting CDR privacy standards and security standards including a description of the process in place to file, monitor, track and restrict access to consumer data;**

    b) **demonstrating that they have the technical capabilities to meet the Standards,**

    c) **adhering to mandatory breach notifications;**

    d) **establishing risk management processes and measures including procedures to deal with security incidents;**

    e) **adhering to trust accounting rules and other measures taken for safeguarding payment service users funds;**

    f) **establishing Internal Dispute Resolution process;**

    g) **membership of an external dispute resolution body i.e. AFCA;**

    h) **processes that meet effective customer consent including testing procedures to demonstrate that customer understand what has been consented to;**

    i) **the collection of statistics/data on performance, transactions and fraud for the use of regulators;**

    j) **ensuring that all primary and secondary uses of any product or service meet a set of ethical standards or principles;**

    k) **no history of data breach or misuse, or of disregard for the law; and**

[18] Para 1.73; subsection 56BF(2)

l) **basic business documentation as similarly required under the EU PSD2 directive, Articles 5(1)(a)-(q).**

4. **Accreditation criteria should ban and/or regulate any price discrimination, algorithmic discrimination and black box algorithms inaccessible to regulators.**
5. **The sale of this data to fourth parties needs to be regulated and overseen under the Open Banking regime, at the very least. We would prefer the practice be banned.**
6. **The concept of sensitive information, as defined under the *Privacy Act 1988* needs to be re-considered to ensure that financial information is appropriately protected.**
7. **Any fees foreseen by the CDR should cover the costs of ongoing administration of the accreditation system not simply the initial accreditation process.**
8. **The Accreditation 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.**
9. **The CDR legislation must ban all screen-scraping and other unsafe data access, transfer and handling technologies.**

CDR data and the CDR consumer

Forms of data

Financial Rights notes that the EDEM envisages that there will be three categories of CDR data.

> *… CDR data that relates to a CDR consumer or has been provided by the consumer, including CDR data that relates to a person's transactions,*
>
> *… CDR data that relates to a product (such as product information data like that contained in a product disclosure statement)*
>
> *… CDR data that is derived from these 'primary' sources.*[19]

Financial Rights supports the broad definition being provided here but it may be important to explicitly states the types of data that this definition is expected to capture, particularly with respect to derived or generated data as referred to above. Specifically this includes:

- value-added data – "data that has been created by a data holder through the application of insight, analysis or transformation of a customer's transaction data to enhance usability and value."[20]

[19] Para 1.51 EDEM

- aggregated data - "where banks use multiple customers' data to produce de-identified, aggregated or averaged data across customer groups or subsets." This can include:
    - de-identified data,
    - anonymised or anonymous data,
    - pseudonymised or pseudonymous data
    - summarised data

There is also another subset of data that will be created from the combination of CDR datasets and *external* non-CDR datasets bought from data harvesters to create a variety of anonymised, pseudonymised or potentially re-identified data.

Delineating these datasets is important for a number of reasons. While these data will, on our reading, fall within the purview of data derived from CDR as per draft subsection 56AF, it is these re-combined re-identified datasets derived from CDR data and held by either accredited CDR participants or non-accredited CDR participants that goes to the heart of safety and security of the system. Breaches, misuse or exploitation of this data will be potentially devastating for consumers and for trust in the CDR regime.

The uses to which certain types of derived data are put to by accredited and non-accredited CDR participants is crucial to the proper functioning of a safe and secure CDR regime. Where there is use of data that has been anonymised and subsequently re-identified through combination with external datasets, is a huge risk.

There will need to be strict rules for each form of data.

The EU GPDR law has simplified the issue by focussing 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.[21] 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 will permit data holders to process anonymous data *and* pseudonymised data for uses beyond the purpose for which the data was originally collected.[22] 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. 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,

---

[20] Page 37 Open Banking Report https://static.treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open-Banking-_For-web-1.pdf

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

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

if de-identified aggregate data is reasonably likely to be re-identified, it cannot be used by the data holder. The EU Article 29 Working Party has yet to release guidance on pseudonymisation and what techniques may be appropriate to use.

The sharing of de-identified aggregated datasets used for the basis of summary data – rather than the summary data itself or genuinely anonymous data as conceived by the EU GDPR - raises concerns for consumers and should be considered carefully by the Government under the Consumer Data Right and Open Banking Regime.

It is important that consumers be able to withdraw consent for the use of data that isn't anonymised or pseudonymised (in the stricter EU GPDR sense) by a data-holder (or participant) in Australia. This data must be destroyed and withdrawn. This is because of the threat to re-identification by the entity or if on-sold to a third party. A right to delete under the Consumer Data Right is essential for this to take place. This would not however apply to genuinely anonymous data.

Further, it is in the interests of full transparency that consumers are fully informed and expressly consent to all uses of aggregated datasets (de-identified or otherwise), and who has access to them, internally and externally. It is likely that consumers will be required to agree to aggregation in order to be able to access some services under the Open Banking regime. It is important that this be the case only if strictly necessary as a primary use of a service.

Identifiable or reasonably identifiable person

Financial Rights notes that under section 56AF(4) a CDR consumer will be :

> *a person to whom the CDR data relates if:*
>
> *(a) the person is identifiable, or reasonably identifiable, from the CDR data; and*
>
> *(b) the CDR data is held by, or on behalf of, either:*
>
> *(i) a data holder of the CDR data; or*
>
> (ii) *an accredited data recipient of the CDR data*

There is an issue arising with a definition that includes a person being "reasonably identifiable, from the CDR data."

There may be a situation where a consumer's data is kept in aggregated form (be it in de-identified, anonymized, pseudonymised form or otherwise) and may not be "reasonably identifiable" at one point in time and then the consumer is re-identified via the CDR data being combined with other external non-CDR data.

Is the person reasonably identifiable from the CDR at this point? Will the consumer be a CDR consumer for the purposes of the Act and be afforded the protections under the CDR regime? What is *unreasonably* identifiable in this circumstance? This is unclear.

The definition may need to be extended in a similar form to that expressed under the EU GPDR – that is a CDR consumer is someone who is identifiable, reasonably identifiable *or is re-identified* from CDR data or its combination with other data.

Recommendations

10. **De-identified aggregate data that is reasonably likely to be used to re-identify a consumer should not be able to be used by a data participant.**

11. **The use of CDR data for the purposes of re-identifying individual consumers should be explicitly banned with significant penalties imposed for attempted and success re-identification of consumers.**

12. **Consumers should be able to withdraw consent for the use of data that isn't anonymised or pseudonymised by a data-holder or participant. This data must be destroyed and withdrawn.**

13. **Consumers should be fully informed and expressly consent to all uses of aggregated datasets (de-identified or otherwise), and who has access to them, internally and externally.**

Consumer Data Rules

Disclosure, use, accuracy, storage, security or deletion of CDR data

Use

Financial Rights notes that there is very little explanation in the EDEM regarding the "use" of CDR data. Financial Rights supports CDR rules being put in place as to the uses CDR data will be able be put to.

Financial Rights notes that the Open Banking Report recommended that

> *The rules would outline that though the data recipient does not need to inform the data holder of all intended uses, there are prescribed uses that should be presented to the customer for permission (consent) to be considered informed.*[23]

We generally support this approach and we would expect that the rules will be flexible enough to evolve over time as uses not currently foreseen may be deemed one of the "prescribed uses that should be presented to the customer for permission (consent) to be considered informed".

The Open Banking Report then moves on to list the uses that it expects would be included in this category:

- *the primary purpose for which the data is being transferred*

[23] Page 136 Open Banking Report, https://static.treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open-Banking-_For-web-1.pdf

- *on-selling of data*
- *direct marketing*
- *transfer of data outside of the Consumer Data Right system, and*
- *transfer of data overseas.*

The rules would also outline that use of lower risk data for secondary purposes must be related to the primary purpose for which the data was transferred, while use of higher risk data for secondary purposes must be directly related to the primary purpose.

The rules would also stipulate that the data recipient and customer cannot be compelled to extend permissions to use with the data holder.

The legislation should also empower the ACCC to create rules that permit certain uses and *prohibit* other uses.

With respect to rules regarding the on-selling of data, we believe the practice needs to be banned outright due to the obvious risks wrought by the increased ease of movement, breach and recombination of sensitive personal financial information.

If, as we expect, the Government will *not* ban the on-selling of data, we would seek the strictest set of rules to be applied. Any business model dependent upon the on-sale of personal data to fourth parties is one that has the potential to sell this data to any and all entities including unscrupulous or disreputable international or Australian parties who have a history of misuse of data through spamming, hacking or other activities that don't meet the law or community expectations.

At a minimum we would expect that specific rules should be established to:

- require genuine consent
- ban on opt-out consents
- prevent the denial of a service for all secondary uses including the on-sale of data
- impose strict liability on the CDR data participant for any breaches of CDR data that arise out of the sale of this data.
- ensure full ongoing transparency
- enshrine the ability to withdraw consent and delete, access to justice and appropriate liabilities for losses subsequent to the sale of the data.

On the latter, third party data recipients must be held liable for any sale to fourth parties where it is reasonably foreseeable that a loss or breach of the Open Banking regime laws and regulations by the fourth party may occur or the accredited party has been negligent. Given data recipients are likely to be profiting from the on-sale of data, they must bear some, if not all, of the responsibility for the sale of the material to fourth parties if a loss or breach of the law occurs. If this is not the case, the Open Banking regime is likely to run into serious issues with consumers who will lose trust and confidence in the regime.

This is, as we read the legislation, not currently the case, but should be.

Similar strict rules should be in place for direct marketing. We note that direct marketing will have its own strengthened "CDR privacy safeguard". This is as it should be. It does however pose the question as to why certain other uses such as on-sale of data do not have their own strict set of CDR privacy safeguards.

We would also expect explicit rules regarding the use of different forms of CDR derived data These rules should cover the use of:

- value-added data
- aggregated data including:
  - de-identified data,
  - anonymised or anonymous data,
  - pseudonymised or pseudonymous data
  - summarised data

As explained above, it is the uses of these different forms of data that will be key to many of the problems that arise.

Finally, there should be rules regarding the use of data not originally consented to. CDR data participants are likely to come up with new secondary and tertiary uses of data. Any new uses of data not originally consented should require additional permission from the consumer before using this data for such new purposes. Strict penalties should be in place for those CDR participants who do not gain such consent and do move to use this data in new forms. The service should not be denied to the consumer for not consenting to such new uses.

Recommendations

14. The practice of on-selling data needs to be banned.

15. If the Government does not ban the practice, a privacy safeguard should be introduced to address the issue. A strict set of rules should be to the practice addressing:

a) genuine consent

b) a ban on opt-out consents

c) prevention of the denial of a service for all secondary uses including the on-sale of data

d) strict liability on the CDR data participant for any breaches of CDR data that arise out of the sale of this data.

e) full ongoing transparency

f) the ability to withdraw consent and delete, access to justice and appropriate liabilities for losses subsequent to the sale of the data.

16. Rules regarding the use of data not originally consented to should be in place.

Consent

The EDEM states:

> *An important feature of the CDR is the consumer's consent to the disclosure of the CDR data. Consumer data rules will be made to provide guidance to both CDR consumers as well as other participants in the CDR system on the matters that have to be satisfied in order to demonstrate that consent was obtained and the CDR consumer understood what it was they were consenting to. The rules will prescribe the process for obtaining consent and how to ensure that consent is genuine. However, it is not intended to make this element of the CDR system so complex as to discourage participation. The role of the consumer data rules is to balance the sensitivity of the CDR data with the need for security, efficiency and convenience.*

Genuine consent is not simply an important feature of the CDR it is the entire lynchpin upon which the CDR succeeds or fails. Genuine consent should, and inevitably will be, the central feature for all data arrangements and privacy standards across the economy moving into future – not simply for designated sectors

As can be seen throughout this submission genuine consent is central to almost every protection and safeguard being proposed for the CDR under the current draft legislation. Without it, consumers will:

- be subject to the lower protections of the APPs when consumer are impelled to consent to providing their CDR data to non-accredited parties who are subject to the APPs;
- be subject to no protections at all under the APPs when consumer are impelled to consent to providing their CDR data to non-accredited parties who are individuals who are not subject to the APPs;
- not be able to avoid direct marketing; and
- not be able to stop the on-sale of their data to fourth parties.

What is genuine consent?

As Financial Rights understands it, this question will be considered by the ACCC in the development of its draft rules for the CDR in September 2018. It is however critical to understand what genuine consent is now in order to fully consider the current legislation and its impact upon consumers.

Article 4 of the EU GPDR defines consent as:

> *any freely given, specific, informed and unambiguous indication of the data subject's [consumer's] wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*

The ACCC should define genuine consent similarly.

The EU has finalised guidelines on consent.[24] These guidelines provide significant further details to the above concepts including examining a multitude of situations and concepts to enable genuine consent to be effective. The guidance 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. We agree with this.

We believe that, at a minimum the ACCC, must introduce the following rules to define genuine consent. That is, consent 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.

Anything less than this will leave consumers open to exploitation, abuse, identity theft, actual theft, spamming and more - all of the nasty issues that Australian consumers currently face.

We believe that the legislation as it currently stands leans too hard on consent to protect consumers from exploitative, abusive or unsafe behaviour from non-accredited parties. Specifically the reliance on genuine consent to protect the interests of consumers who port their data out of the CDR regime to non-accredited parties and subject themselves to lower privacy protections is ill-concieved and will lead to inevitable problems.

Opening the door to non-accredited parties to gain access to CDR data is a recipe for disaster.

While we accept that "the role of the consumer data rules is to balance the sensitivity of the CDR data with the need for security, efficiency and convenience"[25] the balance should not be at a point *where* consumers are encouraged to disclose their data to others without genuine consent, as defined above, being in effect. Given the clear and present risks involved, Government must err on the side of security and protection over convenience to the

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

[25] Para 1.95 EDEM

detriment of the consumer's individual interest. In other words, the interests of business should not trump the interests of consumers to maintain their privacy. Any CDR regime that does not institute a genuine consent regime will be placing the interests of business over that of consumers.

Recommendations

17. **In seeking a "balance" to the consumer data rules, the interests of business should never be able to trump the fundamental interest of consumers to maintain their privacy.**

18. **Genuine consent must be defined as:**

    a) **freely given, absent of any element of inappropriate pressure or influence upon the consumer preventing them from exercising their free will including:**

        i. **any imbalance of power;**

        ii. **the presence of any conditions via for example, the bundling of consent of necessary and unnecessary uses;**

        iii. **the conflation of several purposes without consent for each specific use; and/or**

        iv. **detriment to the consumer if consent is withdrawn or refused;**

    b) **specific including clear separation of information related to the obtain of consent for different data processing activities;**

    c) **able to be constrained according to the customer's instructions including easily withdrawn with immediate effect and deletion of data;**

    d) **fully informed, transparent and fair,**

    e) **time limited, and**

    f) **an unambiguous indication of wishes via an affirmative act from the consumer.**

Deletion

Financial Rights notes that the consumer data rules, accreditation and data standards may develop rules on the deletion of CDR data: subsections 56BB, 56BC, 56BD, 56BE, 56BF.

There is however little information in the legislation or the EDEM about the scope of such deletion rights. The key questions for consumers will be: Will a consumer be allowed to delete their data with:

- the original data holder
- the subsequent data holder

- any on-sold data holder?

It is our understanding from reading the Open Banking Report that no general right to delete will be mandated – given "the fact that individuals currently have no right to instruct deletion of their personal information under the Privacy Act."[26] This is further made clear from the fact that there is no specific privacy safeguard relating to a right to delete under the draft CDR.

The Open Banking Report however recommended that regulators should be provided with a range of remedies to enforce the CDR including directions powers for the deletion of data.[27] It is our understanding that this is likely to be considered for the CDR rules. It is also our understanding that the ACCC will, more specifically, consult on deletion rights where:

- use or transfer permissions are invalid;
- where use permissions are spent; and
- where a data recipient loses the necessary level of accreditation.

However, it is our understanding that, depending on a data recipients' use case and subsequent consent terms for the continued use of data after the expiry or withdrawal of consent, that a data recipient will be able to hold on to personal CDR data with no ability for the consumer to be able to request that information to be deleted. It has been put to Financial Rights that such a right to delete would breach contractual arrangements, the CDR data (in lieu of or in addition to a purchase price) being the consideration for the contract.

Clearly the EU have been able to leap this low hurdle. The EU's GDPR Article 17 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)
- 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)

---

[26] Recommendation 4.3, Page xv. *Open Banking Report*. APP 11.2 states that where:

> *(a) an APP entity holds personal information about an individual; and*
>
> *(b) the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and*
>
> *(c) the information is not contained in a Commonwealth record; and*
>
> *(d) the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information;*
>
> *the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.*

[27] Page 31, *Open Banking Report* https://static.treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open-Banking-_For-web-1.pdf

- the individual objects to the processing of data – including direct marketing purposes and profiling: Article 17(1)(c) & Article 21
- the data was unlawfully processed: Article 17(1)(d)
- there is a legal requirement for the data to be erased: Article 17(1)(e)
- the consumer is a child at the time of collection: Article 17(1)(e) & Article 8

There are also exceptions to this right in the EU, which include:

- exercising the right of freedom of expression and information: Article 17(3)(a)
- for compliance with a legal obligation, e.g. again as mentioned above a bank keeping data for seven years: Article 17(3)(b)
- for reasons of public interest in the area of public health: Article 17(3)(c)
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes: Article 17(3)(d)
- for the establishment, exercise or defence of legal claims: Article 17(3)(e)

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*:[28]

As mentioned however, the *Open Banking Report*, demurred on making a recommendation on the basis that the right does not exist under the current *Privacy Act*.

We believe that this reasonable expectation held by consumers remains.

Consumers do not want the situation where their data has been used by a company – with or without consent – and that company holds on to that data to use for secondary purposes, either in aggregated or de-identified form where there is any possibility of re-identification.

This expectation is also increasing as consumers become more and more aware of and literate regarding the extent their own personal data is being used and misused by companies.

The recent news that UK company Cambridge Analytica legitimately gathered some personal data from Facebook accounts and concurrently illegitimately gathered other people's data, and then, when found out and were requested to delete the data, did not, has raised public consciousness over the potential for data to be misused. Combined with the never-ending list of significant and high-profile data breaches at Equifax, Ashley Madison, Yahoo, Red Cross to name a few and the privacy concerns raised in the context of the recent census and MyHealth Data controversies, the desire on the part of consumers to control their data via strengthened regulations is becoming stronger and stronger every day.

The Government will be opening consumers up to serious consequences if the right to delete is not embedded within the regime from the very beginning. It risks undermining trust and

[28] 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"

confidence in a system it is promoting as the future. If a right to erasure is not included future headlines will likely include the names of accredited and non-accredited CDR entities rather than Facebook and Cambridge Analytica.

A CDR regime that does not provide a deletion right will be one that is hobbled from the start. Consumers will rightly remain highly cynical of any regime that allows CDR data participants to hold on to their data after they leave a service. This fundamental lack of trust and confidence in the regime from the start will lead many to avoid or opt-out of the CDR regime and the potential improved functionality that it promises.

Similarly, Financial Rights strongly recommends that in line with its recommendation that the APPs be reviewed with stronger privacy protections created, that as a part of this review that a right to deletion/right to erasure be introduced into the privacy laws. This would include a thorough re-think of APP 11 with the removal of the "reasonable steps" test removed as a minimum.

Further Financial Rights recommends that a right to deletion be embedded or hardcoded in to the CDR legislation, not as a part of the set of rules but as a fundamental Privacy Safeguard, built into the legislation not the CDR rules developed by the ACCC. We believe that the EU GPDR standard sets a solid benchmark from which to implement such a safeguard.

If, against the advice of almost every privacy advocate in Australia, it is decided that the CDR regime

Financial Rights provides further detail on any right to delete with respect to direct marketing below.

Finally Financial Rights reiterates that there is a fundamental problem with implementing any form of right to deletion with the CDR rules, accreditation and standards, when there is an ability for non-accredited parties to gain access to CDRs where consumers will not have the same privacy safeguards or the non-accredited parties will not be subject to the same rules. This is a crucial flaw when considering the impact of a non-accredited party holding on to CDR data and the ability for this data to be breached, exploited or abused in any way.

Recommendation

19. If the CDR regime is to be implemented without a general right to deletion existing under the *Privacy Act* or APPs, a privacy safeguard should be implemented to establish such a right.

Fees

Financial Rights notes that the CDR rules may also establish fees in relation to the disclosure of certain class or classes of information under the CDR: subsections 56BC(d) and (e) and 56BD(d) and (e).

We wish to make clarify that these fees should be paid by the data holder or participant directly, not by a consumer.

It needs to be remembered that while a data holder may have added value to the data via analysis – it still remains the consumer's data, of which it would hold no value at all. Consumers should retain some rights to this data despite work being done to the data through analysis or otherwise.

Recommendation

20. Any fees established should be paid by the data holder or participant directly not by a consumer.

Incidental or related matters

Financial Rights notes that consumer data rules may be developed for:

> *circumstances where persons are relieved from compliance with the consumer data rules that would otherwise apply to them*[29]

It is unclear what sorts of circumstances are imaged here. We would hope that compliance is strictly enforced and there are few circumstances where this would occur.

Process for making consumer data rules

Financial Rights notes that the EDEM states that:

> *The ACCC must also consider the regulatory impact of the proposed consumer data rules. While it is important that the consumer data rules enable a safe use of consumer data, this must be balanced with the likely regulatory burden arising from the rules. The ACCC will weigh each of these factors when both advising the Minister about designation and when making consumer data rules.*

We believe that safe use of consumer data must be paramount and should not be played off against any notion of regulatory burden. While such burden should be considered as one of many factors, it should not sit side-by-side to the paramount notion of safe use of data.

If a business cannot create a business case taking into compliance costs with regulations that ensure that data is used safely and privacy protections are built in by design from the start, then that is a business that really has no place in a modern economy. Government should not be facilitating the development of businesses that create unsafe data environments. We believe the FinTech sector would not want this either, otherwise in the long run no one will trust their services.

[29] EDEM Para 1.103, Schedule 1, item 1, subsection 56BH(b).

Recommendation

21. The safe use of consumer data must be paramount and should not be played off against any notion of regulatory burden. While such burden should be considered as one of many factors, it should not sit side-by-side to the fundamental notion of safe data use.

Dispute resolution

The successful implementation of a CDR regime is dependent on the development of a strong consumer complaints approach that provides easy, straightforward access to justice.

We note that:

> *the consumer data rules may require CDR participants to have internal or external dispute resolution processes that either relate to the consumer data rules or meet criteria which are outlined in the consumer data rules. [Schedule 1, item 1, subsections 56BH(f) and (g)]* (our emphasis)

Financial Rights believes that rather than "may" require, the CDR rules must require CDR participants to have internal or external dispute resolution processes. Properly functioning IDR and EDR processes is essential for consumers to have access to justice when things go wrong.

We note that the *Corporations Act 2001* requires that an AFS licensee (s912A(1)(g) and 912A(2)) and an unlicensed product issuer or an unlicensed secondary seller (s1017G), *must* have a dispute resolution system available for customers that meet the requirements of RG 165.[30]

We see no reason why a similar requirement be established for the CDR regime. We recommend that the CDR draft legislation at subsection 56BH(f) and (g) be amended to reflect such a requirement.

We acknowledge that there may be smaller CDR participants and individuals whose ability to establish an IDR process may be more limited but we would again direct Treasury to the requirement of all AFSL license holders are expected to maintain an appropriate IDR process.

[30] ASIC, *Regulatory Guide 165 Licensing: Internal and external dispute resolution*, May 2018 https://download.asic.gov.au/media/4772056/rg165-published-18-june-2018.pdf

> *We also need to ensure that financial service providers, credit providers, credit service providers and unlicensed COI lenders, regardless of their size or business, are able to handle complaints or disputes internally in an efficient, timely and effective manner (our emphasis).*[31]

The same expectation must be applied to all CDR participants regardless of size. We note too that Regulatory Guide 165 explicitly allows tailoring of IDR procedures to the size of a business.[32]

Further we believe that the RG165 should act as a template starting point for the establishment of rules for IDR and EDR.

We strongly support the intention to empower existing external dispute resolution schemes such as the Australian Financial Complaints Authority (AFCA) be recognised by the OAIC as the EDR scheme to handle privacy and consumer data right related complaints arising in the Open Banking section of the CDR regime. AFCA should be able to receive, investigate, facilitate the resolution of, make decisions and recommendations for, and report on, complaints about acts or practices of their members that may be an interference with the privacy of an individual.

Recommendation

22. The CDR rules must require all CDR participants, big and small, to have internal or external dispute resolution processes as is in place for all Australian Financial Services Licensees.

23. We support AFCA being recognised by the OAIC as the EDR scheme to handle privacy and consumer data right related complaints arising in the Open Banking section of the CDR regime.

Regulation of the CDR system by the ACCC and the OAIC

Financial Rights continues to support a government-led, multiple regulator model with the Australian Competition and Consumer Commission (**ACCC**) as the lead regulator of the Consumer Data Right.

Financial Rights notes that the legislation will establish a dual regulatory regime:

[31] RG165.43, ASIC, *Regulatory Guide 165 Licensing: Internal and external dispute resolution*, May 2018 https://download.asic.gov.au/media/4772056/rg165-published-18-june-2018.pdf

[32] RG165.68, ASIC, *Regulatory Guide 165 Licensing: Internal and external dispute resolution*, May 2018 https://download.asic.gov.au/media/4772056/rg165-published-18-june-2018.pdf

The ACCC will take the lead on issues concerning the designation of new sectors of the economy to be subject to the CDR and the establishment of the consumer data rules. The OAIC will take the lead on matters relating to the protection of individual and small business consumer participants' privacy and confidentiality, and compliance with the CDR privacy safeguards.

While in theory we support the Office of the Australian Information Commissioner (**OAIC**) as the lead on matters as outlined above, we remain seriously concerned with the OAIC's ability to act in this capacity.

As we have submitted to the Open Banking consultations we have had extensive experience in dealing with the OAIC's complaints process in a number of representative complaints. In general, the complaint handling process that we have experienced has been lengthy, haphazard and opaque. The following are some of the procedural deficiencies that we have experienced:

- *Lack of procedural clarity:* We have not been given an overall explanation of how complaints would proceed from the outset, nor have we been told what the steps toward a determination would be, or the estimated timeframes for the various stages of a complaint.
- *Non-transparency:* In one complaint, we were made aware of discussions that the Privacy Commissioner had with opposing parties regarding one of our complaints, including regulatory guidance that the Commissioner gave to representatives of the opposing party on issues of the complaint to which we were never made privy. We asked for transcripts of relevant meetings or at least a written summary of the issues discussed but we were never given anything.
- *Confidentiality:* Financial Rights has found that it has been unclear what parts of the complaints process were confidential and what parts were not confidential. A statement needs to be sent at the start of a complaint process by the OAIC to both parties to clarify this matter. The complaint process should be transparent.
- *Lack of timeliness:* Financial Rights has experienced significant delays between communications with the OAIC, had meetings cancelled with limited notice, and multiple deadlines given to opposing parties to respond to our complaints were ignored and unenforced. The opposing party in a series of complaints did not formally respond to any of them until eight months after Financial Rights lodged them with the OAIC. We have experienced delays of up to two years.
- *Unreasonable conciliation:* We were also made to attend two separate conciliation meetings even though we made it clear in writing and verbally that we did not believe our complaints could be resolved in that manner, and we were unable to compromise on behalf of all the consumers that we represented in the proceedings.

Given the deficiencies in the OAIC process described above, we believe that AFCA should be empowered to handle all privacy-related complaints related to open banking CDR data. It should be able to receive, investigate, facilitate the resolution of, make decisions and

recommendations for, and report on, complaints about acts or practices of their members that may be an interference with the privacy of an individual.

We also foresee a great variety of complaints arising from the Open Banking Regime which will not relate to privacy. Consumers will complain about services that have not been provided as advertised, about delays in receiving data or services, about errors in data (or perceived errors in data), and about just general customer service failings.

The boundaries between complaints regarding data misuse, privacy and other breaches will be unclear to most consumers using Open Banking products and services. And given the Government's desire to decrease confusion in the financial services complaints space and create a centralised one stop shop, it makes sense to ensure that that confusion is not brought back into this space by having the OAIC be the complaints handling body.

It is critical that the accreditation criteria must include provisions that make membership of the AFCA compulsory.

Recommendations

24. **We support the ACCC acting as the lead regulator in a government led, multiple regulator model which include AFCA and the OAIC to administer and enforce the expansive Consumer Data Right.**

25. **AFCA should be the central point for receiving complaints with respect to privacy breaches and all other issues with respect to the Open Banking aspect of the Consumer Data Right. It should be able to receive, investigate, facilitate the resolution of, make decisions and recommendations for, and report on, complaints about acts or practices of their members that may be an interference with the privacy of an individual.**

26. **The accreditation criteria should include provisions to ensure membership of the AFCA be compulsory for all CDR participants**

CDR Privacy Framework

As detailed above, the CDR Privacy Framework is created a new level of strengthened privacy protections for CDR data that match, but are improvements upon, the Australian Privacy Principles. This inherent from the existence of the new CDR privacy safeguards and is stated as such at 1.169:

> *A more prescriptive approach has been taken to the design of the privacy safeguards to ensure the proper use, access, disclosure or transfer, storage and deletion of CDR data*

As has been acknowledged, a strong privacy framework is essential to the proper functioning of the CDR.

An online survey[33] of nearly 4,500 adults in the UK stated found that the top reasons for not using open banking were:

- Security and misuse of data: 31%
- Invasion of privacy 19%
- Finances are not complex enough to benefit – 18%:

Furthermore there has been little evidence of any benefits to consumers of the Open Banking System:

> *"The additional benefits consumers are going to get in exchange for sharing their financial data remain unquantified and elusive," he says. "Many in the industry have decided this is the right thing to do, without really weighing up what consumers want and need. I personally think there has been a lot of hot air, and the air just got hotter with the Facebook and Cambridge Analytica scandal." Ewen Fleming, financial services partner at Grant Thornton*[34]

Surveying the digital behaviours of 1004 Australian consumers over the past 12 months, CPRC found that 70% were uncomfortable with basic data, such as purchase histories and location data, being shared. Over 85% opposed personal information, such as phone contacts and messages, being shared.[35] The survey also found that the Majority of Australians do not want companies sharing their information for secondary purposes.[36]

We believe the approach being taken with the draft legislation in reflecting the current APPs to be flawed. Aside from the fact that we believe a review of the Privacy Act and APPs is necessary before the establishment of a CDR regime take place, reflecting the APPs in the 12 privacy safeguards simply embeds the outdated and antiquated approach under the Privacy Act and APPs with a few tweaks.

Additionally, there seems to be an assumption that many fundamental privacy safeguards will be left to the rules to spell out. We think this is the wrong approach and a total re-think is required.

While we support many of the proposed Privacy Safeguards – and we address each one separately below – we believe there is a requirement to include a series of additional fundamental safeguards to ensure the proper functioning of a safe CDR regime in a modern economy based on huge technological change.

---

[33] Raconteur, Open banking fails to get consumer buy in, 2 May 2018 https://www.raconteur.net/finance/open-banking-fails-get-consumer-buy

[34] Raconteur, Open banking fails to get consumer buy in, 2 May 2018 https://www.raconteur.net/finance/open-banking-fails-get-consumer-buy

[35] CPRC, Research: Australian consumers 'soft targets' in Big Data economy, 13 May 2018,http://cprc.org.au/2018/05/13/research-australian-consumers-soft-targets-big-data-economy/

[36] CPRC, Fact Sheet: Data protection rules are failing Australian Consumers, April 2018, http://cprc.org.au/wp-content/uploads/Fact_Sheet_-_Data_Protection_Rules_Failing_Australian_Consumers-1.pdf

These include:

- The right to deletion/erasure/right to be forgotten
- Privacy by design
- Right to restrict purposes
- Right to object to processing
- Right to not be evaluated on the basis of automated processing

This submission will first address the proposed safeguards and then provide commentary on these further privacy safeguards.

Consideration of CDR privacy

Privacy Safeguard 1 – open and transparent management of CDR data

Privacy Safeguard 1 is essentially the requirement to have a privacy policy (similar to APP 1). There is really is no significant difference that bolsters the APP 1 requirement.

We believe that this needs to be strengthened to include the following information in a CDR data management policy:

- ***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.
- ***the categories of recipients with whom the data may be shared.***
- ***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

27. Privacy Safeguard 1 should be strengthened to include:

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

    b) the categories of recipients with whom the data may be shared.

    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.

Privacy Safeguard 2 – Anonymity and pseudonymity

Financial Rights notes that Privacy Safeguard 2 is again a straightforward reflection of APP2 with no increase in rights. Further we note that it is the view of Treasury that:

> *… as the first sector to be designated as a CDR sector is likely to be the banking sector, it is expected that the ACCC will make consumer data rules which prohibit the use of a pseudonym for this sector. Consumers are not able to deal with their bank via a pseudonym and it would not be appropriate to enable them to do so within the CDR system*

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

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

Collecting CDR Data

Privacy Safeguard 3 – Collecting solicited CDR data

Privacy safeguard 3 applies to those people who hold accreditation. Presumably accreditation will require meeting CDR rules, which will include rules regarding genuine consent.

We believe though that the centrality of consent should be acknowledged as so important that either a separate privacy safeguard be introduced regarding consent or that reference should be made to consent in the collecting of solicited data under the proposed Privacy Safeguard 3

The privacy safeguard should ensure that a CDR data entity must not collect personal information unless the entity can demonstrate that genuine consent has been received from the customer as defined under the CDR rules. As we have recommended above, consent should 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 obtain 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.

Financial Rights notes again the reference at 1.190 to person holding CDR data as a non-accredited entity. We reiterate our objections to this approach.

Privacy Safeguard 4 – Dealing with unsolicited CDR data

Financial Rights supports draft Privacy Safeguard 4 to ensure that a data recipient who has received unsolicited banking data must destroy as soon as practicable. This is a significant improvement upon APP 4 and APP should be similarly updated.

It is critical that non-accredited entities that receive unsolicited CDR data also 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.

Recommendation

29. "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.

Privacy Safeguard 5 – notifying the collection of CDR data

The reasonable steps standard under the current APP 5 is in no way appropriate for the CDR regime. While the draft CDR legislation states that a person "must take steps" rather than "must take reasonable steps", the steps are those outlined "in the consumer data rules" which could very well fall back on to "reasonable steps" as a standard.

We cannot support this. This standard must be modernized and CDR participants must be *required* to notify, with these notifications acknowledged and recorded. If there is to be any building of trust and confidence in the Open Banking system and the use of consents for the collection of personal information, it is critical that genuine actual notification and disclosure be embedded into the regime.

Joint accounts

We note that the EDEM envisages CDR rules requiring that "each holder of a joint account be notified when collection occurs pursuant to an authorization to transfer data to that account."[37]

While we generally support 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, 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.

Why is this important? 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.*

[37] Pata 1.194 EDEM

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.[38]

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:

- 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;
- preventing access to joint financial assets, such as a joint bank account, for the purposes of meeting normal household expenses;
- demanding disclosure of a person's credit card details and/or passwords;
- demanding cash;
- preventing access to online banking or purchasing;
- preventing someone from 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 it may prevent 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

30. 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.

[38] 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

Privacy Safeguard 6 – use or disclosure of CDR data

A CDR data participant should demonstrate that any secondary use is directly related to the primary purpose. This link between the primary and secondary must not be spurious or trivial. There must be a clear, demonstrable link between the secondary purpose and the primary purpose.

Further, as we have argued above:

- the on-sale of data should be strictly regulated
- genuine consent needs to implemented
- consent should be able to be easily withdrawn and
- the data must be able to be deleted at the consumer's direction.

Recommendation

31. CDR data participant should demonstrate that any secondary use is directly related to the primary purpose

Privacy Safeguard 7 – Use or disclosure of CDR data for direct marketing by accredited data recipients

Financial Rights believes that significant restraints must be placed upon CDR data holders, accredited CDR participants and accredited CDR participants on the disclosure or use of CDR data for direct marketing purposes.

The current APP 7 is manifestly inadequate.

At a minimum must be in accordance with their genuine consent as defined above.

We note that the proposed CDR privacy safeguard 7 will not apply to data holders. We think that it should. Again the easiest way for this to be the case is to review and update the APPs.

For the sake of full transparency, consumers should have the right to know exactly who their data is being shared with and what it is being used for. This information should be made available via a detailed list and included in the consent. If this changes over time, this should be updated and further consent sought.

Moreover, the refusal of consent for marketing purposes should not be used to punish or penalise a customer, nor should it be used to refuse service to a customer.

Recommendation

32. CDR privacy safeguards should apply to data holders.

Privacy Safeguard 8 – Cross border disclosure

Financial Rights believes 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

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

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

Integrity of CDR data

Privacy Safeguard 11 – Security of CDR data

It is unclear whether CDR data provides to a data recipient for a particular purpose

The example at 1.18 refers to Nick instructing his bank ZAP to transfer his credit account information to four other banks in order to test the offers they may be able to offer him.

What is the circumstance though if Nick were to go to CreditCheck app – an accredited CDR data participant - who will automatically test the offers of all banks to find the best deal. In this

case, after decided to remain with ZAP bank, does CreditCheck app have to delete the transaction data? The short answer from the legislation as we read it is – it depends on what Nick has consented to with CreditCheck and what CreditCheck are allowed to do under the CDR rules. It is clear from consultation with Treasury that they expect CreditCheck to be able to retained.

This remains concerning

Correction of CDR data

Privacy Safeguard 12 – correction of CDR data

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 Privacy Safeguard 12 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 modernized and CDR participants must be *required* to correct as soon as practicable.

We note too that there is the possibility for the inclusion of a statement but it remains unclear whether this is a statement from the company or the consumer? We would want the Consumer Data Rules to allow consumers to provide a statement if they do not agree with the assessment of the data participant.

Recommendations

35. **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.**

36. **The Consumer Data Rules should allow consumers to provide a statement if they do not agree with the assessment of the data participant.**

Further privacy safeguards

Financial Rights believes that the CDR legislation should include the following further privacy safeguards:

- ***The right to deletion/erasure/right to be forgotten***

The right to deletion should be a standalone privacy safeguard. Financial Rights goes into more detail above under the Deletion section above.

- ***Privacy by design***

Article 25 of the GDPR implements rules for data protection by design and by default.[39] Privacy by design is a proactive approach to protecting privacy during the design of a project and as well as throughout its life.

Privacy by Design was developed by the Information and Privacy Commissioner of Ontario, Canada, Dr. Ann Cavoukian,[40] The principles were a part of a Resolution by International Data Protection and Privacy Commissioners in 2010; followed by the U.S. Federal Trade Commission's recognition of Privacy by Design in 2012 as one of its three recommended practices for protecting online privacy; and as mentioned, incorporated into the European Commission plans to unify data protection within the European Union.

There are seven foundation principles to privacy by design are summarised by the CPRC summarises as follows:

1. ***Proactive not reactive; preventative not remedial:*** *Be proactive rather than reactive, to anticipate and prevent privacy problems in advance.*
2. ***Privacy as the Default Setting:*** *Personal data is automatically provided with the maximum degree of privacy protection in IT systems or business practices.*
3. ***Privacy Embedded into Design*** *Consider how to embed privacy in the design and architecture of IT systems and business practices rather than a treating privacy protection as a subsequent add-on feature*

[39] Art. 25 GDPR Data protection by design and by default

[40] Information & Privacy Commissioner of Ontario, Privacy by Design, https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf

4. ***Full functionality – Positive-sum, not Zero-Sum:*** *Accommodate all legitimate interests and objectives in a win-win manner, where privacy and security can both be achieved without unnecessary trade-offs.*
5. ***End-to-End Security – Full Life-cycle Projection****: Ensuring strong security measures prior to collecting the first element of information, as well as securely retaining data, and destroying data at the end of the process.*
6. ***Visibility and Transparency – Keep it Open:*** *Businesses practices and technology involved should be subject to independent verification, to assure stakeholders they are operating according to stated promises and objectives.*
7. ***Respect for User Privacy – Keep it User-Centric:*** *Take a user-centric approach by protecting the interest of individuals, for example: offering strong privacy defaults, appropriate notice, and user-friendly options.*

Embedding this approach into the CDR and any other broader re-thinking of the Privacy Act and the APPs is critical to ensure that all businesses demonstrates their respect for consumer data and personal information to provide greater security and privacy protections from day one.

- ***Right to restrict purposes***

Article 18 of the GDPR[41] gives Europeans the right to restrict the processing of their personal data in certain circumstances. Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction, for example they may have an issue with the content of the information held by a company or how they have processed their data. While there may be rights conferred via the CDR rules, a right to restrict purposes should be afforded the status of key privacy safeguard.

- ***Right to object to processing***

Article 21 of GDPR[42] gives Europeans the right to object to the processing of their personal data in certain circumstances. Currently this is materialised under the CDR in part under the direct marketing Privacy Safeguards, but needs to be applied more broadly to the on-sale of data and any other purposes secondary to the primary purpose of the provision of CDR data.

- ***Right to not be evaluated on the basis of automated processing***

Article 22 of GDPR gives Europeans restricts the ability of companies to automatically profile consumers. Article 4 (4) defines profiling as:

> *Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.*

[41] Art. 18 GDPR Right to restriction of processing

[42] Art. 21 GDPR Right to object

Obviously there is a many useful things that can take place by automating some of these processes leading to quicker and consistent decision but it may also lead to serious issues for consumers.

CDR participants should only carry out automated decision-making or profiling if it is:

- necessary for the performance of the contract for the product or service;
- authorised by law; or
- based on the consumer genuine consent.

CDR participants should also be required to:

- to give consumer information about the automated processing or profiling;
- take steps to prevent errors, bias and discrimination; and
- gives consumer the ability to challenge the processing.

Recommendations

37. Further privacy safeguards need to be included in the CDR regime including:

a) The right to deletion/erasure/right to be forgotten

b) Privacy by design

c) Right to restrict purposes

d) Right to object to processing

e) Right to not be evaluated on the basis of automated processing

CDR and CCR

It is unclear how the CDR Regime will interact with the current credit reporting system and the planned introduction of compulsory credit reporting. While the two systems may run in parallel there are a number of circumstances that we can imagine where the CDR may impact on the CCR regime and vice versa.

For example, a new FinTech application by an accredited CDR participant may provide a service that automates comparing and searching for multiple credit products such as credit cards, personal loans, small amount credit contracts etc. The FinTech application may also provide an automated service that institutes multiple applications for credit. The end provider may conduct a credit check at this point. Such applications can be recorded and impact either a credit history and/or a so-called "credit score".

We also foresee credit reporting bureaus (**CRBs**) seeking CDR accreditation to integrate CDR information into their credit scoring algorithms. We note Experion is already a regulated provider in the UK Open Banking sector.[43]

These examples can have serious consequences for consumers. Credit scoring information is becoming more and more important in lending decisions in Australia, and will likely become important in other services as well (i.e. telecommunication services, tenancy). Credit scores are unregulated, opaque and not required to be included on a consumer's free credit reports.

A likely consequence of mandated CCR and access to CDR information via the CDR regime is the increase in the use of credit scores in lending decisions and the use of credit scores to charge certain individuals increased interest rates for credit. Credit scores are the numerical expression of the level of a person's credit worthiness, derived from the information available on a consumer's credit report (presumably). The increased data that will be available about consumers on their credit reports as a consequence of the mandated CCR regime will be incorporated into the current black box algorithms CRBs are using to generate credit scores. These will become clear indicators of consumers that have a less than perfect repayment history. Although this information could and might be useful in responsible lending decisions, our key concern is that credit scores will be obtained by lead generators and marketers to help target direct marketing of toxic or exploitative products to particular vulnerable cohorts that are deemed by a lender to be profitable.

Will consumers really understand the consequences of signing up to a credit reporting bureau service? We would argue most consumer currently have no idea about their role nor their conflicts of interest in providing both free and paid for services. Consumers are regularly misled by the sales pitches for expensive paid for credit reports.

It is clear that this interaction needs to be further considered, and we believe "credit scoring" needs to be examined by government and black box algorithms regulated.

Recommendations

38. Treasury must consider the impact and interaction of the CDR regime with the CCR regime.

39. Government must review and regulate so-called "credit scoring" so that there is more transparency and uniformity around what information is used in the creation of a credit score, who can access credit scores and consumer rights to free access of their own score.

[43] Open Banking (UK), Meet the regulated providers
https://www.openbanking.org.uk/customers/regulated-providers/

Consequential Amendments

Financial Rights notes the following consequential amendments

> *1.273 Subsection 6E(1D) is inserted to the Privacy Act in order that small business operators who hold an accreditation under the CDR regime are treated as an organisation for the purposes of the Privacy Act in respect of information that is not CDR data. [Schedule 1, item 52, subsection 6E(1D) of the Privacy Act 1988]*
>
> *1.274 This amendment means that individuals are assured that there will be no circumstances in which their personal information held by small business accredited data recipients is not protected by either the CDR privacy safeguards or the Privacy Act.*

As noted above – these changes do nothing to protect consumers who have had their CDR data passed on to a non-accredited party who falls outside of the definition of an "APP entity" as currently or subsequently defined.

We strongly believe that all holders of CDR data be they accredited or non-accredited parties must be subject to the CDR privacy safeguards. At a minimum they should be subject to the APPs.

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, Financial Rights Policy and Advocacy Officer on (02) 02 8204 1386.