Financial Rights
LEGAL CENTRE

Submission by the
Financial Rights Legal Centre

The Treasury

Inquiry into Future Directions for the Consumer Data Right

May 2020

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

About the Financial Rights Legal Centre

The Financial Rights Legal Centre is a community legal centre that specialises in helping consumers understand and enforce their financial rights, especially low income and otherwise marginalised or vulnerable consumers. We provide free and independent financial counselling, legal advice and representation to individuals about a broad range of financial issues. Financial Rights operates the National Debt Helpline, which helps NSW consumers experiencing financial difficulties. We also operate the Insurance Law Service which provides advice nationally to consumers about insurance claims and debts to insurance companies, and the Mob Strong Debt Help services which assist Aboriginal and Torres Strait Islander Peoples with credit, debt and insurance matters. Financial Rights took over 22,000 calls for advice or assistance during the 2018/2019 financial year. .

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

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

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

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

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

Monday – Friday 9.30am-4.30pm

Introduction

Thank you for the opportunity to provide input into the Inquiry into Future Directions for the Consumer Data Right (**CDR**).

Financial Rights has been closely involved in the development of the CDR over the past 3 years with submissions provided to:

- Treasury Open Banking: customers, choice, convenience, confidence, December 2017
- Australian Competition and Consumer Commission, Consumer Data Right Rules Framework, September 2018
- Treasury, Treasury Laws Amendment (Consumer Data Right) Bill 2018, September 2018
- Treasury, Consumer Data Right, Privacy Impact Assessment, December 2018 and subsequent independent Privacy Impact Assessment, October 2019
- Data 61, CX Consultation Draft | CDR Consent management and revocation, August 2019
- Senate Economics Legislation Committee, Inquiry into Treasury Laws Amendment (Consumer Data Right) Bill 2018, February 2019
- Treasury, Consultation on Open Banking designation instrument, July 2019
- Senate Select Committee on Financial Technology and Regulatory Technology, Financial Technology and Regulatory Technology, September 2019
- Australian Competition and Consumer Commission, Consumer Data Right: Consultation on how best to facilitate participation of third party service providers, December 2019

as well as numerous other contributions to workshops, roundtables and other consultations.

Financial Rights holds ongoing concerns with respect to the read access implementation of the CDR as it applies to the financial services sector. These concerns are mainly centred on the privacy and security issues that arise from potential access to sensitive financial data by non-accredited third parties. We also hold residual concerns with respect to the impact of the current CDR regime with respect to its application to joint accounts and the potential impact on those Australians who may experience physical or financial abuse or harm.

With these outstanding issues remaining unresolved, and the CDR regime as yet not live, we believe that it is premature to begin an expansion of the CDR when consumer trust has yet to be built. The FinTech sector need to prove themselves able to build trust to protect consumer's interest.

Resources should be directed towards resolving the issues outlined above with respect to read access and build on this. To this end we support a number of the suggestions in the Issues Paper including:

- developing a "consent" taxonomy using standardised language for consents across providers and sectors;
- improve tracking and management of consents;
- promoting of industry cooperation on standards for 'voluntary' data sets *with consumer input;*
- creating of a safe and efficient ecosystem of participants and service providers through the banning of screen scraping;
- introducing a tiered accreditation system, and
- leveraging the CDR infrastructure for other uses such as standardization of regulatory and compliance data across industry and regulators.

Nevertheless this submission outlines our views on approaching the eventual expansion of the CDR to include write access functionality. There has been an unfortunate tendency for technology and commercial interests to lead the discussions for data reform in Australia. This is, in our view the wrong way to approach the *Consumer* Data Right. The consumer interest should drive the further development of the CDR – not the commercial interest of the FinTech or Banking sectors. The consumer needs to be placed back into the centre of the consumer right. Their genuine needs must be considered from their perspective – not from the perspective of what the financial service sector nor the FinTech sector's view of what those needs should be.

Consequently this submission outlines a significant number of issues that banking consumers face on a daily basis, informed by our work on the National Debt Helpline. These issues should act as the basis for his inquiry's thinking on a potential regime and should assist in both identifying the potential benefits of introducing write access and the risks that will need to be addressed or mitigated.

Some of the risks of write access identified in our analysis below include:

- poor consumer outcomes resulting from speedier payment and account initiation processes including more mistaken payments, lower levels of engagement with one's finances, and subsequent higher levels of debt;
- industry profiling for profit with increased economic inequality and financial exclusion as more granular data allows for finer tuned risk segmentation, and less transparent AI-informed decision-making;
- greater potential for the misuse of data including increased fraud risks, errors, incorrect advice or recommendations arising from conflicts of interest through exclusive deals, commissions or other misaligned incentives that place the interest of the accredited third party over the best interests of the consumer.

- significant ethical issues that arise in respect of any increased functionality
- liability and responsibility for payments made.

Finally, this inquiry must examine closely the need to address concerns with the CDR and support proposals to ensure that Australian consumers are protected in an economy based on data. This includes:

- modernising the Australian Privacy Act;
- prohibiting screen scraping;
- developing a legally enforceable AI Ethics Framework; and
- mandating a privacy by design approach to expansion of the CDR and other data related projects.

It is in these ways the original vision for open banking expressed in the 2017 *Open Banking – Customers, Choice, Convenience, Confidence Report* can be fulfilled – one that is customer focussed: for the customer, about the customer, and seen from the customer's perspective.

Summary of recommendations

1. A consent taxonomy with consistent, standardised terminology, processes and experiences must be established and set as rules to ensure that consumers maintain the control over their consents.
2. Any development of standards for 'voluntary' data sets must include consumer voices in the room.
3. Consumer groups and representatives must be supported by government to be able to contribute to the further expansion and development of the CDR.
4. Screen scraping must be prohibited to support the success of the CDR regime.
5. Tiered accreditation should be introduced in a way that does not undermine or compromise consumer privacy, safety and security.
6. All strengthened privacy and consumer protections provided to consumers under the CDR regime should be extended to consumers whose data has been held, misused, abused, exploited or breached by intermediaries or third parties captured in a tiered accreditation regime.
7. Lower tiered accredited parties should also meet CDR Rules appropriate to their role and should have appropriate administrative and procedural protections place to protect consumers.
8. Read only access must be full bedded down and a review undertaken before the CDR functionality is expanded to include write access.
9. The current inquiry needs to place the consumer and their needs front and centre of any consideration in the future to implement rules and standards enabling "write access" under the CDR.
10. Risks identified to consumers must be appropriately mitigated.
11. The remit of the Data Standards Body should be expanded to provide assistance to regulators, self-regulatory bodies and industry to better standardise the data they hold for compliance purposes.
12. This Inquiry endorse and support the need to review and strengthen the Privacy Act to ensure consumers and businesses have the confidence and capacity to engage in the digital world.
13. This Inquiry should endorse the development of an economy-wide prohibition on unfair trading practices, capturing FinTech practices.
14. The FinTech sector should at the very least be required to comply with the AI Ethics Framework or a stronger set of principles endorsed by experts in the field, either via a Code of Practice or under the ACCC CDR Rules.
15. Privacy by design must be embedded into the CDR Rules.

Read access

The Issues paper lists a number of options to expand the functionality of "read" access. Financial Rights provides the following comments on these:

Develop a "consent" taxonomy using standardised language for consents across providers and sectors and How best to enable consumer to keep track of and manage their various consents

Standardisation of consent terms, processes and experiences is critical to ensuring that consumers understand what they are agreeing to when they decide to use a CDR accredited service.

However Financial Rights has concerns that the current Consumer Experience (**CX**) standards and guidelines may not lead to the standardisation required but may lead to some consumers either being misdirected or not understanding their consents and the control they have over them.

CDR Rules 8.1 require data standards to be made for, among others:

- obtaining authorisations and consents, and withdrawal of authorisations and consents; and
- the collection and use of CDR data, including requirements to be met by CDR participants in relation to seeking consent from CDR consumers;

The CX Guidelines produced by the Data Standards Body (**DSB**) contain guidance and examples for putting key standards and CDR Rules into effect. The DSB states on its website that the:

> *CX Workstream emphasises that aligning to the non-mandatory items in the CX Guidelines will help achieve consistency, familiarity and, in turn, facilitate consumer trust and adoption.*

We agree with this statement however we remain concerned that the guidance still provides room to move for individual accredited parties to use their own terminology, their own consent processes and experiences – all in the name of innovation or uniqueness. While the CX standards remain guidelines, standardisation will not necessarily be achieved.

Financial Right's experience in attending CX roundtables is such that we have come away concerned with the approach many FinTechs are taking to the CDR standards and the rules. Much of the work that we witnessed in these workshops has been directed at ways FinTech's can get around rules that have been set including:

- finding, confirming and exploiting loopholes in the rules; and
- developing user experiences that limit consumer ability to control their engagement with the applications and their data including the use of dark patterns - tricks used in apps that make you buy or sign up for things that a user didn't mean to.

There have been many examples of this:

- One FinTech representative stated that they had figured out a loophole to the CDR regime where unaccredited FinTechs[1] can simply ask for people to hand over the data that the consumers themselves request directly from their data holder in a machine readable format. These FinTechs/companies would therefore not have to get accredited. This is in fact the issue that the consumer movement has been warning about in the development of the CDR rules and legislation – leakage of sensitive financial data outside of the protections of the CDR framework. This FinTech asserted that they planned to be exploiting this loophole from 2022.
- Another FinTech representative believed that CDR Data Recipients will be able to offer consumers something in return for consenting to the holding or de-identification of data - that is they plan to have their client FinTechs offer movie tickets, vouchers, cash or other financial incentives to consent to the collection and retention of de-identified data. This fundamentally undermines the concept of consent as detailed under the rules ie voluntary, express, informed, specific as to purpose etc. Will people really be freely consenting to a particular use if that consent is based on an incentive unrelated to the use. There is currently nothing in the Draft Rules to prevent Accredited Data Recipients providing CDR Consumers with a reward or incentive if they provide their consent for the Accredited Data Recipient to de-identify some or all of the collected CDR Data for the purposes of disclosing (including by selling) the de-identified data (in accordance with Rule 4.11(3)(e)).
- As an example of designing the consumer experience to benefit the FinTech over the interests of the consumer, FinTech representatives wanted to obfuscate the consumer's choice in the design of the re-authorisation process. Consumers will at some point need to either re-authorise a FinTech App or cease use of the app. FinTech representatives asserted that the clearest way to ask a consumer whether the consumer wanted to re-authorise something was to provide them with 2 choices: "Modify" or "More info". Not simply "Re-authorise" or "Stop sharing data' (or simply "delete."). This obfuscation is clearly in the interests of the industry rather than the consumer. At every opportunity the FinTech sector representatives sought to build in "friction" to the process of deleting one's data. This seeking of increased "friction" in this case is somewhat ironic given the relentless calls from the FinTech sector to make the CDR, data-sharing and switching "frictionless" transactions. It is only where the Fin Tech sector's self- interest is served, in seeking to hold onto customers and their data, that they see the benefits of friction.

This approach from the FinTech sector is unsurprising: self-interest and pursuit of profit at the expense of the consumer interest drives regulatory arbitrage in most sectors. It nevertheless remains disappointing.

What it requires though is a shift away from the DSB providing mere guidance, towards establishing set of rules outlining a consent taxonomy with consistent, standardised terminology, processes and experiences to ensure that consumers maintain the control over their consents.

[1] Or the clients of Fintechs using their services

Recommendation

1. **A consent taxonomy with consistent, standardised terminology, processes and experiences must be established and set as rules to ensure that consumers maintain the control over their consents.**

The promotion of industry cooperation on standards for 'voluntary' data sets

We support the promotion of industry cooperation on standards for 'voluntary' data sets however we wish to ensure that if these discussions are taking place then there are consumer voices in the room. The 'voluntary' data being referred to here is ultimately consumer data. Consumers need to be involved when the use of their data is being discussed and decisions should not be simply left up to industry alone.

Financial Rights' experience in contributing to the development of the CDR and Open Banking has been that we are usually the sole consumer representative in the room – a room full of banking and FinTech interests – sometimes upwards of 50 to 100 industry representatives.

While there has been some small steps towards bringing the consumer voice into these discussions with survey research reports, and the appointing of a consumer organisation to obtain a broader set of views from different consumer perspectives – these have really only occurred in the last 6 months – well after many key decisions have been made.

Consumer representatives have largely been unable to attend any workshops on because consumer groups generally do not have the resources to be able to attend and contribute. This is particularly the case at a time when Banking Royal Commission recommendations are being implemented (addressing past and current problems with the financial services sector). Contributing to addressing future problems that may arise from the use of consumer data including personal financial data has had to take a back seat for most of the sector,

It is critical that any moves to expand the scope of the CDR support obtaining views of consumers and providing support to consumer groups to provide input into the process – including those groups who work with Australians experiencing financial hardship or other forms of hardship.

Recommendations

2. **Any development of standards for 'voluntary' data sets must include consumer voices in the room**
3. **Consumer groups and representatives must be supported by government to be able to contribute to the further expansion and development of the CDR**

How the creation of a safe and efficient ecosystem of participants and service providers could be accelerated.

For the CDR to succeed and build high levels of consumer confidence and trust in a safe and secure FinTech sector, the outmoded and dangerous practice of screen scraping must be prohibited. The issues with screen-scraping are numerous:

- screen scraping requires unsafe online practices actively deterred by government and industry;
- screen scraping breaches bank terms and/or conditions, whereby losing E-payments Code protection;
- screen scraping is slow, unstable and prone to errors;
- allowing screen scraping to continue undermines the potential success of the CDR;
- allowing screen scraping to continue places Australian FinTech at a disadvantage.

Banning screen-scraping will enable FinTech sector to develop consumer trust. We provide further details of why this in **Appendix A** below, drawn from Financial Rights' submission to the *Senate Select Committee on Financial Technology and Regulatory Technology*, *December 2019*.

Recommendations

4. **Screen scraping must be prohibited to support the success of the CDR regime.**

The scope for use of tiered accreditation to promote broader access without increasing risk

Financial Rights has been a long supporter of a tiered accreditation regime as it will resolve many of the issues regarding privacy and security that we have raised in previous consultations.

The key issue that we have been concerned with is the potential ability for CDR data to be disclosed to, and obtained by, non-accredited third parties. If this occurs, consumers are likely to be subject to decreased levels of protection of their data – protections that are at the heart of the reasons for introducing the CDR in the first place.

This potential remains and is an issue that was recently consulted on (and yet to be acted on) by the Australian Competition and Consumer Commission (**ACCC**).[2] Financial Rights has outlined

[2] ACCC consultation on facilitating participation of intermediaries in the CDR regime, 23 December 2019 https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0/accc-consultation-on-facilitating-participation-of-intermediaries-in-the-cdr-regime

the key issues with allowing non-accredited third parties access to sensitive financial data to this consultation and outlined at **Appendix B**[3]

We remain of the view that non-accredited third parties should *not* be permitted to receive CDR data and that it is inappropriate for any unaccredited third party to receive and hold CDR data. Allowing for such an ability fundamentally undermines the entire point of the CDR regime in promoting safer and more secure data practices, and will likely lead to a lack of consumer confidence in the regime as soon as the inevitable first breach occurs.

It also goes against the Open Banking Review original recommendations that the CDR legislation should be a closed system to prevent any CDR data being provided to any non-accredited entity.

There are a number of ways to resolve this issue including strengthening CDR privacy safeguards through extending these protections to all consumers and their data in all situations. However the key way to resolve this is by creating a new accreditation tier.

The CDR can and should accommodate the use cases of accountants, financial advisors, real estate agents and others by designing an accreditation system that appropriately extends the consumer protections of the CDR to these cases and sets accreditation standards that appropriately reflect the different role played by potential entities who are currently considered non-accredited third parties.

This may involve reduced requirements, but should include all the safety and security requirements that would ensure consumers remain protected.

Tiered accreditation would also deal with issues raised by the use of intermediaries – also consulted on recently by the ACCC.

In designing tiers for both currently unaccredited third parties and intermediaries, consumer data safety and security must be prioritised. It is critical that no loopholes or exemptions are put in place for CDR data holders, recipients or intermediaries to take advantage of Australian consumers or undertake any form of regulatory arbitrage or avoidance.

It is essential that *all* the strengthened privacy and consumer protections afforded consumers under the CDR regime should be extended to consumers whose data has been held, misused, abused, exploited or breached by an intermediary or a third party included in the tiered accreditation regime.

The same strong sanctions and remedy regime should also be applied to non-accredited third parties. These are details in **Appendix B.**

[3] See further details in Financial Rights' Submission to the Senate Economics Legislation Committee Inquiry into *Treasury Laws Amendment (Consumer Data Right) Bill 2018*, February 2018 https://financialrights.org.au/wp-content/uploads/2019/03/192028_SenateCDRInquiry_Submission_final.pdf

Recommendation

5. **Tiered accreditation should be introduced in a way that does not undermine or compromise consumer privacy, safety and security.**
6. **All strengthened privacy and consumer protections provided to consumers under the CDR regime should be extended to consumers whose data has been held, misused, abused, exploited or breached by intermediaries or third parties captured in a tiered accreditation regime.**
7. **Lower tiered accredited parties should also meet CDR Rules appropriate to their role and should have appropriate administrative and procedural protections place to protect consumers.**

Write access

What is write access?

Write access in short allows payment initiation - allowing third parties to be able to make payments from a customer's account on the customer's behalf. We also understand that it can involve account initiation and closure. The UK Open Banking regime has already implemented both read and write access reforms with payment initiation. This is because the UK had an obligation to comply with the EU's Payment Services Directive 2 which requires write access.

Australia chose to develop the CDR through iterations and extensibility which will enable the country to work out complex issues and limit any potential consumer harms. This is a sensible approach and should continue to be the case.

Read access must be bedded down first

We note that the original Open Banking Report stated that:

> *For open banking to succeed customers need a high level of confidence that their data is secure and that it is only being used for the purpose that consent is given. If write access was created before open banking was fully bedded down, that may put its success at risk. Further, while write access has significant benefits, it may take some time for customers to feel comfortable with third parties acting on their behalf … for these reasons it would be premature to consider implementing it at this stage.*[4]

We agree with this view and believe that it is premature to begin an expansion of the CDR when consumer trust has yet to be built through the introduction of a read access CDR.

This current inquiry and the possible extension to "write access" is in our view not being driven by calls from consumers. Very few Australians know what the CDR is let alone the concept of Open Banking. The vast majority of Australians remain in the dark on open banking, with more than three-quarters (77 per cent) saying they do not know about it at the end of 2019.[5]

There is no evidence to demonstrate any great consumer desire for read access let alone write access to Open Banking. This is an extension solely driven by the FinTech sector who claim to know what consumers are wanting and needing, claims that support a case for planned business models.

Further, the FinTech sector have yet to prove themselves able to be trusted to protect consumer's interests. Given the experiences described above in the development phases of the CDR – we continue to have concerns with respect to how FinTechs are approaching the handling

[4] Page 109, The Treasury, Farrell, Scott, Review Into open banking: giving customers choice, convenience and confidence, December 2017 https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking-_For-web-1.pdf

[5] FinTech Business, Most Australians unaware of open banking, 9 December 2019 https://www.fintechbusiness.com/data/1605-most-australians-unaware-of-open-banking

of consumer data. We believe the FInTech sector must prove themselves able to build trust to protect consumer's interest.

The UK FCA have outlined what has developed in the open banking environment[6]:

Table 1 Opening banking services

Envisaged services which have developed	New developments which were not envisaged	Envisaged services which are not yet developed/early stages
Account aggregation	Financial inclusion	Automatic product switching
Account data access to inform lending decision	Protections for financially vulnerable people	Balance transfer management (credit cards)
Personal financial management	Legal aid and welfare support advice	High balance sweeping
SME financial management	Retrospective Gift Aid claims	Cashflow optimisation
Account-to-account money transfer using PIS	Several API aggregation services have entered the market	Interest maximisation
		Merchant payments using PIS
		CBPIIs providing payment services

While account to account money transfer using PIS does appear in the list of Open Banking services that have developed - the UK FCA's state that:

> *most market developments have involved AIS (Account Information Service) business models rather than Payment Initiation Service PIS*[7]

In other words – initial demand for open banking in the UK – where it has arisen at all - is centred on read access use cases rather than read write access use cases.

Despite the lack of any evidence of consumer interest or demand for write access, we recognise the government's interest in exploring this expansion and feel there is no harm to explore the potential benefits and costs of introducing write access – as long as these are fully considered before write access is introduced and read only access is fully bedded down.

Recommendations

8. **Read only access must be full bedded down and a review undertaken before the CDR functionality is expanded to include write access.**

[6] page 8 https://www.fca.org.uk/publication/call-for-input/call-for-input-open-finance.pdf

[7] Financial Conduct Authority Call for Input: Open finance https://www.fca.org.uk/publication/call-for-input/call-for-input-open-finance.pdf

Issues faced by consumers in banking and credit that should inform the development of a write access expansion.

Given the industry-driven nature of the call for write access - we recommend that *this* inquiry take a consumer-focussed approach to the consideration of write access. Rather than starting with the potential use cases, or abilities of write access to drive the discussion on any expansion to the CDR we believe the preferred approach is to start with the issues that consumers face in the current market that could be resolved or exacerbated by any reform.

There has been an unfortunate tendency for technology and commercial interests to lead the discussions for data reform in Australia. What has occurred is that businesses have first identified new technological capabilities, then built business models and business cases based on these capabilities and finally identified the consumer needs that could be addressed by these business models.

This approach ignores the potential use cases that may actually serve consumer interests against the interests of industry. We note that the FCA UK found that there were Open Banking developments which were originally envisaged including uses cases directed at financial inclusion, protections for financially vulnerable people and legal aid and welfare support advice: see Table 1 above. This suggests that consumer needs were not fully explored in the UK before the introduction of the regime.

Consequently - informed by the casework we undertake on the National Debt Helpline - we provide the following list of key issues that banking consumers face on a daily basis. These issues should inform the development of open banking and a write access regime. This is not a complete list by all means but should nevertheless inform this inquiry's thinking on a potential regime and should assist in both identifying the potential pros of introducing write access and the cons that will need to be addressed.

- ***High levels of debt***

  Australians are some of the most indebted people in the world.[8] This is the result of a multitude of factors including easy access to credit (credit cards, mortgages etc), new forms of credit such as buy now pay later services, harmful business models such as pay day lending and consumer leasing, increasing utility costs, low levels of financial literacy and budgeting skills, stagnating wages etc.

  Any CDR based read/write service that may assist in better budgeting, keeping on top of regular bill payments, or actively switching to better deals, consolidating or transferring debts – when done right could assist many Australians. In the hands of independent financial counselling services, improved budgeting and payment processes could be beneficial. However in the hands of for-profit debt vultures or debt management firms,

[8] Australians' record debt is making us work longer, spend less, https://www.abc.net.au/news/2019-10-18/household-debt-leaves-australians-working-longer-spending-less/11608016 18 October 2019

less optimal outcomes could result – exacerbating problems our service already sees in this space.

An expanded CDR may also promote subsequent higher levels of debt by encouraging the sale of additional or higher cost credit, be it credit cards, loans or other lending.

Furthermore, it may encourage higher levels of debt through the use of AI-informed algorithms that introduce increased risk segmentation, price optimisation and inappropriate price discrimination where more financially vulnerable cohorts will be provided credit at a higher cost than other consumers.

- ***Difficulties in closing and opening accounts***

  Closing accounts is an issue faced by consumers that we speak with on the National Debt Helpline with complications and hurdles in place to prevent the loss of customers. These can include having to contact a bank by phone in or in person, no easy way to identifying and dealing with direct debits and recurring payments (see below). These can be time consuming and act as a barrier to switching.

  There are also a number of pros and cons to switching accounts generally. For some, consumers may be able to earn interest at the highest rate. Introductory offers are also provided to many that may be attractive. However there other issues that need to be considered such as closing fees (hidden or otherwise); the loss of other benefits with sticking to an account, or terms and conditions or requirements with a new account that may not be so beneficial to the consumer.

- ***Difficulties in cancelling direct debits***

  Consumers regularly report difficulties cancelling direct debits despite the existence of the Banking Code provisions requiring a bank to cancel a direct debit in a savings/transaction account when instructed by to do so by the customer. Enforcement of and compliance with this section of the Code has in the past been lax. Cancellation has not been prompt in many circumstances – let alone immediate. The new Banking Code does however include stronger commitments in this regard.[9]

  Further, consumers regularly have multiple direct debits established that need to be identified and cancelled. This can be time consuming but also can lead to errors, consumers missing the cancellation of some payments or paying for services they no longer need. These issues are even more difficult when closing and opening an account. We note too that the Banking Code now seeks to address this.[10]

- ***Difficulties in cancelling recurring payments***

[9] Chapter 34, Banking Code of Practice

[10] Clause 134, Banking Code of Practice

Recurring payments are technically different to direct debits despite consumers believing them to be the same in practice. Recurring payments are regular payments on credit or debit card allowing merchants to charge regularly to pay for a good or service. Direct debits are on deposit accounts.

Cancelling recurring payments is an ongoing, intractable problem as yet unresolved by the banks and the payment systems.

More and more people are setting up payment arrangements using MasterCard or Visa numbers on their cards and are actively encouraged to do so by banks through rewards systems. Banks argue that they cannot cancel these recurrent payments and that customers should instead request a chargeback from the credit card company. Both the Banking Code and the COBA Code are silent on the obligations of banks to address customer requests to cancel such recurring payments. Banks have yet to resolve the issue in negotiations with Visa and Mastercard – which has come down to who will pay.

"Write access" may play a role in resolving this issue if applied to these arrangements. If it could then this would be of significant benefit to consumers who face considerable hurdles in dealing with banks and merchants on this matter.

- ***Difficulties in establishing a direct debit***

  Sometimes consumers face hurdles in establishing direct debits in the first place. For example, ANZ has required credit card customers to fax their direct debit details to establish a direct debit to make automatic payments. Embedding ways to make this initiation more streamlined and standardised could be beneficial.

- ***Consumers find themselves in less than optimal accounts***

  Many Australians find themselves paying too much for their mortgage or credit card, or find themselves in a deposit account charging too high a fee. The Financial Service Royal Commission for example found that many people were in inappropriate accounts allowing overdrafts and having high fees.[11] While the banking code has been amended making commitments with respect to the provision of basic banking accounts and requiring banks to be more proactive in identifying vulnerable consumers who may be inappropriate accounts – the issue remains alive for many other consumers experiencing financial hardship.

- ***Hurdles to switching***

[11] See 4. Access to banking services from page 88, Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry: Volume 1, Final Report https://www.royalcommission.gov.au/sites/default/files/2019-02/fsrc-volume-1-final-report.pdf

Levels of switching in the banking sector are low with credit card switching at 17% and home loan switching at 18%[12]. There are a number of behavioural and structural reasons for this including: difficulties with comparison services, lack of ease, brand loyalty etc.

The key harm is that consumers may not be receiving optimal service, lower interest rates or a raft of other features through not switching. There are however risks to switching as touched upon above.

- ***Financial capability - poor budgeting skills and low levels of financial literacy***

  ANZ Research shows Australians have differing attitudes to money and varying levels of financial knowledge and proficiency. People may perform well on some aspects of financial literacy but poorly on others.[13] Similar to the above, improved ability to handle finances or raising engagement levels with their finances could be of use to Australians – if done in the right way with independent and free financial counselling services rather than by debt vultures. The National Strategy for Financial Capability has identified three behavioural areas in which Australians can be empowered to take control of their financial lives:

  - managing money day-to-day;
  - making informed money decisions; and
  - planning for the future.[14]

  There may be a role for the CDR read/write access to improve literacy and capability levels – but there is just as much a risk that consumers rely on the third party apps to undertake financial decision-making for them and counterintuitively disengage with their financial wellbeing.

- ***Difficulties in managing multiple accounts***

  Many banking customers – that is most Australians – no longer simply have a savings account or a mortgage account. They can have large number of accounts including offset accounts, redraw facilities, credit card accounts, etc that require constant juggling of finances.

- ***Ease of making errors in transfers***

  Consumers regularly make errors when transferring funds – a situation that has been exacerbated with the introduction of the New Payments Platform and the instantaneity

[12] https://www.heritage.com.au/switch-to-heritage/~/media/c74a9ea0bda54ba6a9da4f49b0866154.ashx

[13] ANZ Survey Of Adult Financial Literacy In Australia May 2015 Full report of the results from the 2014 ANZ survey https://www.anz.com/resources/3/1/31cbc1fd-9491-4a22-91dc-4c803e4c34ab/adult-financial-literacy-survey-full-results.pdf

[14] https://financialcapability.gov.au/

of transfers. The ePayments Code covers mistaken payments, where the payment is sent to someone other than the intended recipient – however there a number of errors that arise that are not currently covered by the ePayments code – including an error in the payment amount. We see many examples of blame shifting between banks: one bank says that it is the other bank that they are waiting on, and vice versa. At present, there is often little or no recourse, particularly if the person that the money was accidentally sent to has already spent it or transferred it elsewhere.

Write access could improve the process – although it should be noted that the NPP is in place and is expected to fulfill a number of the payment solutions sought. As we understand it there is active development under way to enhance the NPP infrastructure to support payment initiation messages that would provide a customer-controlled, real-time replacement for Direct Debit authorisations.[15] According to Deloittes:

> *Once implemented, these could provide capabilities for payment transactions to be initiated by third parties on behalf of customers. They could also provide customers with the ability to manage the consents they have provided to authorising third parties to access funds and initiate payments from specified accounts. These capabilities would provide a similar if not greater functionality for customers than the payment initiation capability implemented under both the UK and EU open banking regimes.*[16]

However write access could potentially exacerbate and multiply the problems described above. It also raises the potential for increased levels of fraud.

- ***Debt vultures (or Debt Management Firms) not acting appropriately***

  Australians experiencing financial hardship or vulnerability are regularly tempted to use debt vultures including for profit budgeting services, debt negotiation services, credit repairers Part IX debt negotiations usually with poor results. Many of these use tactics that if used under a write access regime in the CDR could supercharge the harms that are currently occurring. For example, personal budgeting services may be more likely to keep your money in your account earning interest (and therefore earn money for themselves) for as long as possible instead of paying your debts when they are due. Customers complain that they are left without enough money to live on. Personal budgeting services may take no responsibility for dealing with creditors if there is not enough money in the account to pay all of your bills.

- ***Price discrimination and risk segmentation***

  Australian consumers are already subjected to inappropriate price discrimination in the lending market with those with higher levels of credit risk charged excessively high interest and pushed into second tier credit markets. The CDR read access has the

[15] NPP Australia,"New Payments Platform Roadmap 2019", 28 October 2019 as referenced in Delloites Open Banking | Payment initiation - completing the vision

[16] Page 5, Delloites Open Banking | Payment initiation - completing the vision

potential to increase levels of price discrimination in this way. Providing write access to potentially now initiate transactions with these providers where increased friction is required to slow down the process is a real risk.

- ***Credit reporting and credit scores***

  Consumers continue to jealously guard their credit rating/score in order to continue to obtain credit – sometimes to their detriment – for example by choosing not to seek a financial hardship variation as it may impact negatively upon their rating even though they need the relief. There may be benefit to some consumers to ensure that all their bills are paid on time in an automatic form through the use of write access technology. However, depending on the algorithms involved, more switching may lead to worsening credit reports and scoring – as would higher incidence and increasing levels of debt.

- ***Financial abuse***

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

  While banks have a series of guidelines and policies in place to deal with many of the issues that arise here[17] – the CDR has yet to grapple fully with the issues of financial abuse beyond the potential for misuse of the CDR for physical or financial harm or abuse under the CDRs Rules 3.5, 4.7, and 4.6. We understand too that the ACC are expected to consult further on joint account rules. Furthermore – the nascent FinTech sector have not grappled with these issues in a thorough way as yet, with no similar guidelines or Code of Practice.

  Write access threatens to super-charge financial abuse unless appropriate constraints and protections are put in place.

[17] Including ABA Industry guideline – Protecting vulnerable customers from potential financial abuse https://www.ausbanking.org.au/wp-content/uploads/2019/05/Industry_Guideline_Protecting_vulnerable_customers_from_potential_financial_abuse2.pdf; ABA Industry guideline – Financial abuse and family and domestic violence policies https://www.ausbanking.org.au/wp-content/uploads/2019/05/ABA_Industry_Guideline_-_Financial_Abuse_and_Family_and_Domestic_Violence-Nov-2016.pdf

Current mooted use cases

While we have touched upon some of the pros and cons of write access as it applies to the consumer issues listed above – it is worth now examining some of the mooted use cases for write access:

- **Payment initiation**

  Automating the payment of bills and invoices on due dates and pay them from chosen accounts without having to go back to the data holder bank will be useful to address a number of the issues above including better budgeting, more regular bill paying, improving credit scores etc.

  However it is critical that this be done so in a manner that promotes good outcomes for consumers. Developing CDR apps to assist free and independent financial counsellors to assist those experiencing financial hardship is qualitatively better than enabling for profit budgeting services with conflicts of interest doing the same.

  Consideration needs to be given to examining business models that are developed that act in ways that may require a financial advice licence, brokers licence or an AFSL, to ensure that the best interests of the consumer are protected when an accredited third party were to initiate payments in service of advice, broking or any other financial service.

- ***Account opening and closing (switching)***

  Automating the opening and closing of accounts to optimise savings and finance management. It could also streamline a process that can be incredibly complicated, difficult and time consuming. But regulatory oversight is required to ensure that the mooted comparison and recommendation results are in fact true and in the best intersts of the consumer. For example, a switching service that recommends opening an account with a cheaper bank account– needs to be free from conflict of interest – that is –the account was not recommended simply because it provides the best kickbacks or commissions for the accredited third party provider.

- ***Funds movement for saving and wealth management***

  Shifting around funds to optimise interest rates is again useful for some people but can involve some risks for others where they may lose benefits accompanying the original bank account or be met with restrictions arising out of the terms and conditions of the new account.

- ***Changes to Identification***

  The issues paper states that it wishes to examine:

  > *whether write access should extend to the ability to change details which identify a customer (and if so, how any associated security risks could be minimised).*

This functionality presumably means that a third party would be able to initiate the change of an address, phone numbers and other personal details in data holder accounts. While this may introduce some convenience for some consumers, there are significant risks in doing so particularly with respect to joint accounts, the potential for financial abuse that may occur through the exploitation of such functionality. This also needs to be considered in the context of Austrac oversight.

Risks requiring for consideration and potential mitigation

This initial analysis above demonstrates that there are significant benefits but also risks that may arise through the introduction of write access to the CDR. We outline these risks below

- ***Poor consumer outcomes borne of speed and less friction***

  Consumers generally seek convenience and speed over security and suitable products. However there are many cases where they do so to their own detriment. Frictionless transactions are already causing significant consumer harm in the online consumer space, for example the ease of accessing payday loans via mobile applications, or an increase in mistaken e-payments.

  Reducing the friction – or put more simply – increasing the speed associated with payment initiation, account closing and opening and transacting without advice increases the chances of harm to a consumer where they would have been better to seek advice from a free and independent financial counsellor or a licenced financial advisor or broker subject to licensing requirements.

  Auto-switching has the real potential to lead to consumers becoming even less engaged with their finances and, over time, unaware of whether the products that they have are still suitable.

  Auto-switching could also lead to consumers becoming focused solely on price over other factors affecting suitability – particularly if there are no best interests duty, no conflict of interest rules or regulatory over-sight on the AI or algorithms.

- ***Profiling for profit: 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 by FinTechs and easier ability to open and close accounts in an instant.

  Customers with certain characteristics will be excluded from certain markets and or provided access at cost. Those experiencing financial hardship are often very profitable to debt management firms and fringe financial service providers 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.

  Even where there are benefits to consumers, there is the potential for some consumer cohorts to be excluded from the benefits of write access including those consumers who

opt out of data sharing, or those who are unable to access or use the CDR such as older Australians. The former receive less advantageous pricing sometimes referred to as 'privacy premium'; the latter are simply structurally excluded.

The more granular the data obtained, the finer tuned the risk segmentation will become. AI-informed decision-making (in terms of provision of financial product or service, the price of a premium, or the level of interest offered) will become less transparent, with the potential for discrimination increased. Without the provision of explanations (both technical and non-technical) AI-informed decision making will not be considered safe and reliable.

- ***Misuse of data***

  Consumers may provide consent to share their data, initiate payments or switching but may not be aware of how their data are ultimately used, leading to uses the consumer had not contemplated or intended.

  There may be increased risks of fraud, if all a consumer's data are available through one single point of entry, or are held by firms with poor system security and governance. Consumers are more and more aware of the impact of the data that they are providing to digital platforms and services and are increasingly concerned about the impact upon their privacy rights and the protections in place about the use or their data.

  Out of date, incorrect or incomplete data being shared could result in incorrect advice or recommendations, a switch to an inferior product or the wrong price. This could be exacerbated through conflicts of interest arising out of exclusive deals, commissions or any other misaligned incentives that will place the interest of the accredited third party over the best interests of the consumer.

- ***Consent and transparency***

  The consent regime under the CDR has yet to be tested in the real world, may be wildly inconsistent (see discussion above) and may need refining to ensure that consumers are genuinely providing consent.

  Accredited parties will need to provide sufficient information, in a clear format, to enable the consumer to both understand how their data is being used, what will happen when payments are initiated (and other write access functions) to make an informed decision.

  Closed proprietary algorithms could 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 poor consumer outcomes through the creation of potentially biased and discriminatory algorithms

  A consumer's focus on switching to a different financial product or service may mean that other factors, such as privacy and security concerns, feature less prominently in

their decision making. As a result, it is possible some consumers may not appreciate the full implications of their decision to share their data.

- ***Data Ethics***

  There are significant ethical issues that arise in respect of any increased functionality of the CDR. Data must be used in an ethical manner as must the services provided. Ethical issues will arise in the use of machine learning or artificial intelligence (AI). There is currently no mechanism to ensure consumers understand exactly how their data will be used in this respect, how decisions are made or how value will be extracted from it. It is critical that FinTechs at the very least adhere to the Department of Industry, Innovation and Science's set of voluntary principles to be used when designing, developing, integrating or using AI systems[18] as well as any future regulation of this space envisioned by the Australian Human Rights Commission inquiry into Human Rights and Technology. The FinTech sector must be proactive and establish codes of practice to both improve consumer confidence and to establish sets of consumer protections that are not necessarily enunciated under the law – ensuring a mixed regulatory system. The sector must act now – not wait to react to any consumer harms that will inevitably arise.

- ***Liability and responsibility for payments made***

  Payment initiation and other write access functions raises the key issue of who is responsible when there is an error, mistake or a dispute arises. It must be clear where liability sits if things go wrong.

  Currently if a data holder provides information to another person or allows that person to access information, in good faith and complying with a CDR system requirement, the data holder providing the information is protected from liability under section 56GC of the Competition and Consumer Act.

  Similarly, where the accredited third party acts to initiate a write access function and the data holder complies in accordance with the CDR rules, the data holder would be protected from liability.

Recommendation

9. **The current inquiry needs to place the consumer and their needs front and centre of any consideration in the future to implement rules and standards enabling "write access" under the CDR.**
10. **Risks identified to consumers must be appropriately mitigated.**

[18] https://www.industry.gov.au/data-and-publications/building-australias-artificial-intelligence-capability/ai-ethics-framework/ai-ethics-principles

Leveraging Consumer Data Right infrastructure

RegTech: Leveraging Consumer Data Right infrastructure for regulation

We believe that there is a role for the Data Standards Body to assist regulators in their supervisory and data gathering roles, and supporting businesses in managing their regulatory compliance.

Regulatory Technology or RegTech is the application of technologies to streamline and improve the way businesses manage regulatory compliance.

In the financial services sector, banks, insurers and other financial services providers across the board are expected to provide more and more data to regulators under enhanced regulatory monitoring.

For example, the Australian Prudential Regulation Authority (**APRA**) and the Australian Securities and Investments Commission (**ASIC**) recently undertook a program to collect and publish performance data on life insurance claims and disputes. This involved two years of work aimed at developing with industry higher-quality, more consistent and transparent data about the life insurance industry. It also involved standardising definitions with the sector facing significant challenges including:

> *Different insurers currently record the necessary data in different ways, in part because they have differing claims and complaints practices. Insurers also adopt different terminology and data definitions. This makes achieving comparability difficult, and can also give rise to data quality issues as data may need to be manually extracted and manipulated.*
>
> *Legacy products and systems (with varying constraints and complexities) present challenges to the extraction of data and are complex and expensive to update to support new data collections. They increase the level of complexity in the system, and in particular cause significant administrative challenges…*
>
> *Life insurance products are inherently complex and the operating environment (including distribution channels) is also complex, with a wide range of different structures and products in existence. This makes like-for-like comparability a challenge.*

We expect that ASIC and APRA will need to expand their ability to gather similar information in both the life insurance sector and the general insurance sector but also across the financial services sector. This is key information that is not necessarily consumer data but drawn from consumer data that is useful to regulators in their supervisory role and consumers in being better informed (of say claims rations, complaints rates and outcomes).

We note that ASIC have developed a data strategy and Regulatory Transformation Program – both a part of what is called 'One ASIC'. It comprises key activities that seek to improve data collection, management and governance; enhance processes; make interacting with ASIC simpler; and cut red tape to help improve compliance. The DSB could play a role to assist ASIC in the future of this project.

RegTech can be used to develop market analyses that examine actual consumer outcomes in the finance services market. Regulators should be provided with detailed market monitoring tools with transaction detail data for everything from default data, claims, sales and quotes data to transaction information.

The information gathered by regulators could also be used to provide information to empower consumers and promote competitive markets. For example, claims data insurance could be used to provide claims ratios for consumers at point of sale. Interest rate practices could be provided to consumers to seek out better deals.

The information gathered via RegTech could also assist:

- evaluating existing and proposed public policies
- evaluating affordability and availability of financial services and products and
- competition issues.

We believe that the Data Standards Body's remit should be expanded to provide assistance to regulators and industry to better standardise the data they hold for compliance purposes.

Compliance matters is not always a matter for external regulation but also self-regulation. The financial services sector has a large number of codes of practice – many of which are about to become enforceable following implementation of Royal Commission recommendation 1.15: see Exposure Draft of *Financial Sector Reform (Hayne Royal Commission Response—Protecting Consumers (2020 Measures)) Bill 2020: FSRC rec 1.15 (enforceable code provisions).*[19]

Industry also requires standardisation of compliance to these codes and consistency of data has been an issue. We believe that the Data Standards Body could also play a significant role in establishing data standards for industry in this context.

Recommendation

11. The remit of the Data Standards Body should be expanded to provide assistance to regulators, self-regulatory bodies and industry to better standardise the data they hold for compliance purposes.

[19] https://treasury.gov.au/consultation/c2020-48919f

Consumer Protections

Outside of any protections specifically needed to mitigate issues arising from any future write access functionality, Financial Rights has provided a number of suggestions during the development of the CDR regime to improve consumer protections and outcomes, that we wish to raise again. These include

- modernising the Australian Privacy Act;
- prohibit the dangerous practice of screen scraping;
- prohibiting unfair trading practices;
- developing a legally enforceable AI Ethical Framework;
- mandating privacy by design.

Modernise the Australian Privacy Act

We strongly support broader reform of the Australian privacy regime to better promote and support the interests of consumers by placing their interest front and centre of the regime over the profit-driven interests of FinTechs, digital platforms and businesses to retain, use and exploit private information.

We note the Government's response to the Digital Platform Inquiry includes the announcement of a review of the Privacy Act to

> *"…ensure it empowers consumers, protects their data and best serves the Australian economy. A review will identify any areas where consumer privacy protection can be improved, how to ensure our privacy regime operates effectively for all elements of the community and allows for innovation and growth of the digital economy…"*

The review will consider a number of ACCC recommendations that the Government has supported in principle including:

- updating the "personal information" definition: Recommendation 16(a);
- strengthen notification requirements: Recommendation 16(b);
- strengthen consent requirements and pro-consumer defaults: Recommendation 16(c);
- enable the erasure of personal information: Recommendation 16(d),
- introduce direct rights of action for individuals: Recommendation 16(e), and
- increase penalties for breaches: Recommendation 16(f).
- introduce a statutory tort for serious invasions of privacy: Recommendation 19.

If consumers are to have any trust in digital commerce moving into the future, these broader reforms are essential.

As the Government has stated:

Data is the resource that powers much of this activity, and it is being created and collated at an unprecedented scale. The capacity to process this data is also improving, providing us with greater insights and information than ever before.

While the benefits of digital services and technology are vast and will continue to grow, we must also be aware of, and respond appropriately to, the risks that are presented so that consumers and businesses have the confidence and capacity to engage in the digital world.

We recommend that this inquiry not undertake its work in a vacuum and support the application of stronger privacy laws and other mooted reforms to the FinTech sector.

Recommendations

12. **This Inquiry endorse and support the need to review and strengthen the Privacy Act to ensure consumers and businesses have the confidence and capacity to engage in the digital world.**

Prohibit the dangerous practice of screen scraping

As we have noted above - for the CDR to succeed and build high levels of consumer confidence and trust in a safe and secure FinTech sector, the outmoded and dangerous practice of screen scraping must be prohibited.

Full details of this position are provided at **Appendix A**, drawn from Financial Rights' submission to the *Senate Select Committee on Financial Technology and Regulatory Technology*, *December 2019*.

Prohibit unfair trading practices

The Final Report of the Financial Services Royal Commission identified six norms of conduct, one of which was to 'act fairly'.[20] The norm of fairness is also recognised in the objective of the *Competition and Consumer Act 2010* (Cth) which is 'to enhance the welfare of Australians through the promotion of competition and *fair trading* and provision for consumer protection.'

Just as the concept of fairness must be applied in the "real world" financial services sector, the same must be applied to the FinTech sector.

Enacting an economy-wide prohibition on unfair trade practices as recommended by the ACCC in the Digital Platforms Inquiry will ensure fairer outcomes for consumer across the real world and digital economies.

[20] Royal Commission into Misconduct in the Banking, Finance and Superannuation Industry, Final Report, page 8.

This has been supported by Government who has backed the work of Consumer Affairs Australia and New Zealand on exploring how an unfair trading prohibition could be adopted in Australia to address potentially unfair business practices.[21]

We raised with this issue with the ongoing *Senate Senate Select Committee on Financial Technology and Regulatory Technology* and provide full details of why unfair business models and practices in the data space need to be prohibited. For a full exploration of this see **Appendix C**.

Recommendations

13. **This Inquiry should endorse the development of an economy-wide prohibition on unfair trading practices, capturing FinTech practices.**

Develop a legally enforceable AI Ethics Framework

We believe that this inquiry should examine the ethics of AI-informed decision-making in the Finsnacial Services and FinTech sectors that are likely to be introduced with an expanded CDR and Open Banking.

Financial Rights has raised many of these issues with the recent *Senate Select Committee on Financial Technology and Regulatory Technology*, *December 2019*. This is available to read at **Appendix D**. We have also raised many issues relevant to this current inquiry with the Australian Human Rights Commission's Human Rights and Technology Inquiry.[22]

However we wish to emphasise the need to embed principles within the FinTech sector that ensure the promotion of ethical value creation rather that value appropriation.

The Department of Industry, Innovation and Science recently developed a set of voluntary principles that are designed to be used when designing, developing, integrating or using artificial intelligence (AI) systems.[23]

---

[21] Regulating in the digital age Government Response and Implementation Roadmap for the Digital Platforms Inquiry, December 2019, https://treasury.gov.au/sites/default/files/2019-12/Government-Response-p2019-41708.pdf

[22] Submission to the Australian Human Rights Commission's (AHRC's) Human Rights and Technology Issues Paper, 2018 https://financialrights.org.au/wp-content/uploads/2018/10/181002_HRTechIssuesPaper_Submission_FINAL.pdf

[23] https://www.industry.gov.au/data-and-publications/building-australias-artificial-intelligence-capability/ai-ethics-framework/ai-ethics-principles The eight principles are: (1) Human, social and environmental wellbeing: Throughout their lifecycle, AI systems should benefit individuals, society and the environment. (2) Human-centred values: Throughout their lifecycle, AI systems should respect human rights, diversity, and the autonomy of individuals. (3) Fairness: Throughout their lifecycle, AI systems should be inclusive and accessible, and should not involve or result in unfair discrimination against individuals, communities or groups. (4) Privacy protection and security: Throughout their lifecycle, AI systems should respect and uphold privacy rights and data protection, and ensure the

While the establishment of this voluntary framework is a good start it is clear that this will not be enough moving into the future.

The FinTech sector should act now and agree to at the very least adhere to the AI Ethics Framework via a Code of Practice or a stronger set of principles endorsed by experts in the field. Alternatively, the ACCC CDR Rules should be amended to require CDR participants to meet these standards.

Recommendations

14. **The FinTech sector should at the very least be required to comply with the AI Ethics Framework or a stronger set of principles endorsed by experts in the field, either via a Code of Practice or under the ACCC CDR Rules.**

Mandate a Privacy by Design approach

Article 25 of the EU GDPR implements rules for data protection by design and by default.[24] 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,[25] 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.*

security of data. (5) Reliability and safety: Throughout their lifecycle, AI systems should reliably operate in accordance with their intended purpose. (6) Transparency and explainability: There should be transparency and responsible disclosure to ensure people know when they are being significantly impacted by an AI system, and can find out when an AI system is engaging with them. (7) Contestability: When an AI system significantly impacts a person, community, group or environment, there should be a timely process to allow people to challenge the use or output of the AI system. (8) Accountability: Those responsible for the different phases of the AI system lifecycle should be identifiable and accountable for the outcomes of the AI systems, and human oversight of AI systems should be enabled.

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

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

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 treating privacy protection as a subsequent add-on feature*
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 Protection****: 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 expansion of 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. We note that the recent CovidSafeApp was developed using these principles.[26]

We believe that the use of this approach should be mandated by the government in the expansion of the CDR and the development of all CDR based products and services moving into the future.

Recommendations

15. Privacy by design must be embedded into the CDR Rules.

[26] "In developing the App, the Australian Government has taken a "privacy by design" approach, including by taking steps to minimise the collection of personal information and to limit who will be able to access App Information." Page 3, Para 1.4 Department of Health The Covidsafe Application Privacy Impact Assessment 24 April 2020 https://www.health.gov.au/sites/default/files/documents/2020/04/covidsafe-application-privacy-impact-assessment-covidsafe-application-privacy-impact-assessment.pdf

Concluding Remarks

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

Kind Regards,

Karen Cox
Chief Executive Officer
Financial Rights Legal Centre

Appendix A

Extract from the Joint Consumer Submission to the Senate Select Committee on Financial Technology and Regulatory Technology, December 2019

Prohibit the dangerous practice of screen scraping

For the government's CDR to succeed and build high levels of consumer confidence and trust in a safe and secure FinTech sector, the outmoded and dangerous practice of screen scraping must be prohibited.

What is screen scraping?

Screen scraping is the process by which screen display data is obtained and translated from one application to another. It usually involves a consumer providing their log-in credentials (eg username and password) to a third party (such as a payday loan operator) who then uses these to access the data held by another party (such as a bank) via a customer-facing website. Consumer data is then collected from the website for various purposes.

Screen scraping is ostensibly used in the lending sector to undertake responsible lending checks and is prevalent throughout the small amount credit contract market. The case studies below demonstrate the flaws and risks when this technology is relied on by lenders to undertake lending checks:

Case study Annabel's story - C196186

About 2 years ago, Annabel got a loan a payday lender for $1,500. The lender uses a data aggregator with screen scraping technology to obtain required information for responsible lending checks.

In the 90 days before this loan was obtained, Annabel had entered into 2 other Small Amount Credit Contracts (**SACC's**) with the payday lender and was a debtor on 6 SACC's in total. This fact was noted in the loan application.

Annabel borrowed a further $700 in 2018.

Last September, Annabel's Centrelink benefit changed from DSP to Newstart, and Annabel was unable to afford repayments at the fortnightly rate of approximately $150.

In examining Annabel's situation, Financial Rights obtained documentation from the payday lender which was based on the use of a data aggregator's screen scraping tool.

The report was riddled with inaccuracies including:

- Incorrect calculations with respect to her net monthly income which inappropriately took into account lump sum cash advance payments she received from Centrelink and assumed they were additional regular income.
- Missing information with respect to EFTPOS payments.

Source: Financial Rights Legal Centre

Case study Jane and Bernie's story

Jane and Bernie (names changed) were a couple with 4 dependent children. Their income derived from Centrelink and Bernie's casual job.

In late 2016 Bernie decided to purchase a car and was referred to a broker. The broker failed to properly explain the agreement they were jointly entering (even though the car was for Bernie) and Jane did not understand the relationship between the broker and the lender.

While the finance company appears to have roughly assessed Jane and Bernie's incomes correctly, it appears to have used only a one-page account scraping document pertaining to an account in Bernie's sole name, which was submitted in the loan application, to verify expenses. The finance company does not appear to have obtained copies of bank statements for Jane and Bernie's joint accounts or Jane's sole accounts at the time, which would have shown whether the loan was unaffordable for Jane and Bernie.

Both the broker's loan application and finance company's assessment appear to significantly understate Jane and Bernie's living expenses, with the expenses listed on the lending assessment document totalling even less than that on the loan application. The finance company appears to have applied an arbitrary benchmark that was lower than both the Henderson Poverty Index (HPI) and Household Expenditure Measure (HEM) benchmarks for that quarter.

They soon fell into arrears on the loan as the loan was not affordable for Jane and has caused her substantial hardship.

Source: Consumer Action Law Centre

In the Australian market screen scraping technology is provided by the likes of the US-based Yodlee, Adelaide based Proviso and Sydney-based Basiq.

Screen scraping that Financial Rights see produces documents that break down incomings and outgoings in consumer accounts detailing categories such as wages, Centrelink payments, SACC loans, Groceries, Fees, Telecommunications expenditure etc.

The information provided can be useful for lenders if used responsibly and appropriately but there are a significant number of problems with the practice – many of which can be and are now resolved by the CDR.

What is wrong with using screen-scraping technologies?

The problems with screen scraping data aggregators are numerous and include the following:

Screen scraping requires unsafe online practices actively deterred by government and industry

The basic procedural premise of screen scraping is it requires a consumer to hand over their password and username details in order to access and analyse their data. This is an inherently unsafe online practice and is exactly the opposite to every other piece of online safety and security advice provided to Australians by both the online industry and in government advisories.

For example, ASIC's Money Smart website tells people that that:

> *"Don't tell anyone your passwords - a legitimate business or company should never ask you for your password."*[27]

The Australian Government's StaySmartOnline website states:

> *"Keep your passwords secure by taking measures to protect them: Don't share your passwords with anyone."*[28]

The Australian Government's my.gov.au initiative also recommends that:

> *To protect your account: don't share your myGov sign in details with anybody else*[29]

It is a dangerous practice to hand over one's password details because encouraging such a practice makes passwords and security information more vulnerable to breach and can lead to people being scammed, people having their identities or money stolen or worse. It is also dangerous to hand over password material to FinTech and financial services providers.[30]

Case study Zed's story

Zed (name changed) was trying to negotiate a hardship variation with Zip Money. Zip Money were aware that Zed had physical issues, an acquired brain injury and was taking

[27] https://www.moneysmart.gov.au/scams/avoiding-scams

[28] https://www.staysmartonline.gov.au/protect-your-business/doing-things-safely/passwords-business

[29] https://my.gov.au/mygov/content/html/security.html

[30] We note that FinTech Australia report that "between 10-50 per cent of potential customers baulk at handling over their passcode" https://treasury.gov.au/sites/default/files/2019-03/c2017-t224510_FinTech_2.pdf. This is because it is an inherently unsafe practice and consumers are well-advised not to do so.

medication that affected his cognitive ability. They also knew that a financial counsellor was assisting him. Despite this, Zip Money contacted Zed directly stating that in order to assess his variation they would need copies of his bank statements. Zip Money stated that to make this "easier" he could supply his banking credentials to the third party company Credit Sense. Concerned about what to do, Zed got in touch with his financial counsellor for advice.

Source: Consumer Action Law Centre

We are aware of financially vulnerable clients providing log-in details to payday lenders, only to have the payday lender use the log-in details later to identify when a consumer is getting low on cash and subsequently directly advertise to that consumer. This has the effect of exacerbating financial hardship.

The Financial Services Royal Commission made explicit recommendations against the hawking of superannuation and insurance noting that "the practice has long been unlawful because it too readily allows the fraudulent or unscrupulous to prey upon the unsuspecting."[31] A ban on hawking should also capture online hawking that can result from unsafe practices such as screen scraping.

The asymmetry of power and information between the payday lenders with access to someone's financial information and that individual is immense. Even if the 'hawker' was not fraudulent or unscrupulous, the customer may be ill-informed, unsuspecting, or lacking knowledge and is not prepared to critically evaluate the offer.

Provisions set out in the *Corporations Act 2001*[32] prohibit offering financial products for issue or sale during (or because of) an unsolicited meeting or 'cold' telephone call - but these scenarios imply that the hawker is a human exercising agency.

We encourage this Committee to recommend amending both the law, and ASIC regulatory guidelines for hawking (RG 38 (2005)), to capture digital or online hawking.

Our organisations regularly hear of other dodgy practices:

Case study Edward's story - C197644

Edward was searching for good rate deals for credit on the internet. Edward found a rate on a lender's website and he then contacted them for further information. The lender then sent him an email. Edward responded and provided information to begin a process he believed would lead to him being provided with an offer. As a part of this process

[31] Page 13, Final Report Volume 1, Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, https://www.royalcommission.gov.au/sites/default/files/2019-02/fsrc-volume-1-final-report.pdf

[32] See sections 736, 992AA and 992A

Edward was required to provide his details to his bank account and to obtain his credit report in order for him obtain his "tailored interest rate."

Before he knew it Edward had been approved for a $15,000 loan with the money deposited into his account. Edward had only been shopping around and had not expected to be provided with the money - merely an offer. The lender refused to rescind the contract until they had been told that he had contacted Financial Rights. In the meantime Edward had in fact found a better deal and wanted to go with this other lender.

Source: Financial Rights Legal Centre

If the advice of the Australian Government is to *not* hand over log in details, it is inconsistent and dangerous to allow Australian FinTech companies to ask for and receive log in details to highly sensitive bank accounts.

Screen scraping breaches bank terms and/or conditions, whereby losing E-payments Code protection

Providing access to one's banking data using screen scraping technology amounts to a breach of the terms and conditions of a customer's bank account, and places customers at risk of losing their protections under the E-Payments Code.

The E-payments Code states:

> *11.2 Where a subscriber can prove on the balance of probability that a user contributed to a loss through fraud, or breaching the pass code security requirements in clause 12: (a) the holder is liable in full for the actual losses that occur before the loss, theft or misuse of a device or breach of pass code security is reported to the subscriber*

The rationale for this is clear. Sharing a password is as detailed above, an inherently unsafe practice and it would be a moral hazard to allow consumers to provide such details and not be liable for the loss that occurs as a result.

Banking Terms and conditions make it very clear that providing a password to a third party breaches the terms and conditions of the facility. For example ME Bank states:

> *Account aggregation services – warning*
>
> *6.31 Some companies provide an account aggregation service that allows consumers to view account information from different institutions on the one web page. To use an account aggregation service, you are usually required to give the service provider your account details and your access codes (for example, your username and password and/or PIN).*
>
> *6.32 We do not endorse or authorise the use of account aggregation services in connection with your account*
>
> *6.33 Please remember that if you break your agreement with us not to disclose your PIN to another person, you will be liable for any transactions on your account made using your PIN.*

> *There is also a risk that information about your account obtained by an account aggregation service provider or its employees may be misused.*[33]

FinTech Australia has however argued that rather than prohibiting the unsafe practice of screen scraping, the e-Payments Code itself should be updated to make it clear that customers are not liable for monetary losses, where they supply their passcode to a company accredited by ASIC.

> *Working closely with stakeholders to develop agreed passcode security and complaints handling standards, which is expected to legitimise existing industry safeguards and inform the ASIC accreditation approach.*[34]

There are a number of fundamental problems with this suggestion.

First encouraging people to hand over passwords and usernames runs counter to all other security advice provide by the Australian government as outlined above. Even if it was safe to hand over log-in details in the Fin Tech context – which it is isn't – it would undermine safe practices in all other online contexts.

And second accrediting screen scraping by ASIC undermines the entire point of the accreditation system under the CDR regime.

The government's CDR was developed for this very purpose. It is nonsensical to develop a parallel system to serve the interests of a small number of legacy FinTechs who are unwilling to change their business model to meet the higher standards and security requirements of the CDR regime.

Screen scraping is slow, unstable and prone to errors

In addition to being unsafe screen scraping is generally considered slow, with estimates that what would take 5 to 10 minutes to undertake via screen scraping takes seconds under Open Banking.[35] FinTech Australia also acknowledges that there are faster technological solutions available.

Furthermore screen scraping is fundamentally unstable and technology breaks down regularly. Screen scraping scans the existing consumer-facing web portals of financial providers, which means that if there is a small change to a website it can create stability issues for those screen scraping tools. Open banking APIs do not have this issue.

Case study Gavin's story - C196186

[33] Pages 18-19 Everyday Transaction Account Terms and Conditions https://www.mebank.com.au/getmedia/c0bf2e3a-30a3-492c-9690-c5397dc0a486/eta_terms_and_conditions.pdf

[34] Submission to Open Banking Inquiry, September 2017 https://treasury.gov.au/sites/default/files/2019-03/c2017-t224510_FinTech_2.pdf

[35] Kelly Read-Parish, Open Banking vs. Screen Scraping: looking ahead in 2019, 4 January 2019 https://www.finextra.com/blogposting/16494/open-banking-vs-screen-scraping-looking-ahead-in-2019

Gavin has payday loans totaling $4,000. In December last year he applied for loans with a payday lender where he was declined on two applications but accepted into two other loans.

Gavin has struggled to pay the loans as he has Child Support of $400 per fortnight and rent. Gavin pays $400 a fortnight to the payday lender with fees of $80 for each loan per fortnight.

Financial Rights has begun representing Gavin but upon looking at the data aggregation provided for responsible lending purposes, it was riddled with errors – including categorizing his café payments for coffee as rent.

Source: Financial Rights Legal Centre

Allowing screen scraping to continue undermines the potential success of the Consumer Data Right

There are advantages to both consumers and to financial services and FinTech companies in using third party providers to obtain bank statement information including the ease and speed of providing bank statement information for responsible lending and other appropriate purposes.

However this is very the reason the government's Consumer Data Right was established – to provide a fast, safe, and secure process to access personal and financial data.

The Consumer Data Right is fundamentally a right to port and transfer one's own personal financial data – similar to screen scraping – but in a safe environment "ensuring …high levels of privacy protection and information security for customer data"[36]

Without a ban on screen-scraping, there is very little incentive for businesses such as payday lenders and debt management firms to use CDR accredited software over screen scraping technology.

FinTech Australia have stated that:

> *"many fintech companies are happy with existing screen scraping solutions, and are likely to continue to use these solutions even when alternative technology is available."*

Joining the CDR regime involves justifiable higher regulatory hurdles, obligations and costs to ensure that consumers can have trust and confidence in those who they are sharing their sensitive financial data with.

Allowing the practice of screen scraping to continue therefore encourages those who seek to access financial data not to join the CDR – particularly those who may not meet the fit and proper person test under the accreditation regime, those who may not wish to spend the money

[36] 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/

(approximately $50,000 -$100,000) on gaining and maintaining accreditation[37] or those who see no reason to have to do so.

It has been suggested that FinTechs will naturally want to become accredited in order to gain the confidence of their potential users. While there are many service providers, for example, who may seek reputational legitimacy, many will not. Additional hurdles, regulations, obligations and costs introduced by an accreditation process will remain unattractive to many of these businesses, some of whom already skirt the regulations currently in place.

If the prevalence of irresponsible lending in the payday lending market is anything to go by, there is arguably little financial, reputational or other incentive for many FinTech players to seek accreditation if they can continue relying on old technology – even if it is riddled with problems.

Financially vulnerable people desperate to access credit via a service that uses old and unsafe screen scraping technology will not concern themselves with the nuances of privacy protections to do so. If that means engaging with non-CDR accredited entities like dodgy payday loan operators still using screen scraping, those financially vulnerable people will do so and end up with lower privacy protections than customers seeking loans from CDR accredited lenders.

Personal responsibility is commonly brought up as an argument to maintain the ability for consumers to choose to use services that use screen scraping technologies. But when consumers are excluded from accessing mainstream credit and the only provider will use screen scraping technology – there is no true choice here for a consumer to decide between obtaining credit and giving up privacy and other rights. Genuine consent is absent where the power is held by the provider.

Even non-financially vulnerable consumers may hold misplaced trust in a financial advisor or accountant who uses screen-scraping technologies. 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 is therefore more deserving of trust.[38] The same principle could very well apply with respect to greater disclosure and transparency with respect to the application or lack of privacy safeguards. If the scandals in financial advice, mortgage and insurance broking that led to the Financial Services Royal Commission are anything to go by, this will continue to be the case.

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.

This ultimately undermines the potential success of the CDR regime to ensure great consumer protections and increase confidence in the sector.

---

[37] Page 9, Senate Select Committee On Financial Technology And Regulatory Technology Issues Paper, https://www.aph.gov.au/~/media/Committees/fintech_cttee/Issues%20Paper%20-%20FinTech.pdf?la=en

[38] 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 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."*

Allowing screen scraping to continue places Australian FinTech at a disadvantage

Screen scraping is a near defunct technology that the rest of the world is moving beyond.

Screen scraping has been banned in the UK and the EU under the Payment Services Directive 2 (**PSD2**). There is currently a 6 month transition ending 14 March 2020.[39]

The reasons for this are essentially to ensure UK customers are provided with safer and strong authentication processes under Open Banking. Screen scraping technology has been accepted as yesterday's technology and encouraging the Australian sector to continue to use the technology in the face of our own Open Banking system will place our industry at a disadvantage internationally as resources keep being poured into a defunct and out of date standard.

Banning screen-scraping will enable FinTech sector to develop consumer trust

Like all sectors of the financial services industry – and indeed the broader economy - the FinTech sector will thrive or remain stunted on the basis of consumer confidence in the products and services they provide. The FinTech sector though is particularly vulnerable to the threats borne of the nature of their offering – that is the potential for their services to be and be seen to be unsafe, insecure, manipulative or downright dangerous.

It is therefore in the sector's interest and the Australian economy's interest to build a safe and secure, forward thinking regulatory environment that promotes consumer confidence and engagement. Banning screen-scraping is fundamental to this transformation.

Recommendations

16. The Inquiry should recommend that screen scraping be prohibited to support the success of the Consumer Data Right regime.

[39] FCA, Strong Customer Authentication, 2 September 2019, https://www.fca.org.uk/firms/strong-customer-authentication

Appendix B:

Extract from the Financial Rights Submission to the Australian Competition and Consumer Commission Consumer Data Right Consultation on how best to facilitate participation of third party service providers, February 2020, Pages 6-11.

Permitting CDR data to be disclosed to non-accredited third parties

8. What types of non-accredited third parties should be permitted to receive CDR data? Why is it appropriate for those types of third parties to be able to receive CDR data without being accredited?

It is our strong view that no non-accredited third parties should be permitted to receive CDR data and that it is inappropriate for any non-accredited third party to receive and hold CDR data.

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

> ***Recommendation 2.7 accreditation***
>
> *Only accredited parties should be able to receive Open Banking data. The ACCC should determine the criteria for, and method of, accreditation.*[40]

The reasons for a closed system were detailed as follows:

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

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

> *The UK has decided to limit access only to accredited third parties known as 'whitelisted parties'. A bank would only comply with a customer's request to transfer their data to a third*

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

party if that party is 'whitelisted'. This limitation of access reduces risk and gives users greater confidence in sharing data. The EU's PSD2 also contains an accreditation process.

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.

Accreditation for all those parties interested in using CDR can be done so on a sliding scale if need be. However critically it would ensure that consumers taking part in the CDR will be able to avail themselves of the strengthened privacy safeguards afforded under the CDR regime.

Varying levels of privacy protection

The introduction of the CDR regime has created multiple levels of privacy standards for different people that will apply at different times to consumers seeking protection, security and redress when something goes wrong. They include:

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

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

1. CDR data accessed and held by non-accredited parties who are "APP entities"[41] will be subject to the APPs, not the CDR privacy safeguards.
2. CDR data accessed and held by non-accredited parties who are not "APP entities" will neither be subject to the APPs nor the CDR privacy safeguards but only general consumer protections and law.

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

The risks bear repeating.

- *Fewer, if any, security requirements increases the likelihood of a breach:* Non-accredited third parties holding CDR data are more likely to be breached, given stronger security requirements under the CDR will not apply to them;

[41] 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

- *Identify theft:* If breached sensitive financial data can be used for identity fraud by a bad actor;
- *Material theft:* If breached sensitive financial data can be used to access funds by a bad actor;
- *Fewer consumer rights:* If anything were to go wrong, the protections and rights afforded by the CDR will not apply.

We note that the ACCC states in the consultation paper that:

> *The ACCC recognises there are existing mechanisms that facilitate the transfer of data from consumers to third parties.*

In other words – if non-accredited third parties were to be able to access CDR data – then this is really no different to what is occurring now.

It may be true that third parties are be able to access financial data currently but the entire point of the CDR – its entire reason for being - is to make the access to and transfer of high sensitive financial data safer, more secure and consistent. It is meant to improve what occurs by encouraging consumers to share their data within a safe and secure system with the confidence and assurance that their privacy will be protected. Allowing the easy, faster transfer of CDR data to non-accredited third parties without the same consumer protections as expressed under the CDR privacy standards is to fundamentally undermine the entire point of the CDR and will lead to both poor outcomes for consumers and has the very real potential to undermine the success of the CDR altogether.

Any decision to allow non-accredited third parties 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.

Solutions

The key principle the CDR regime must meet with respect to the use of CDR data is that consumers who choose to use and pass on their CDR data are afforded all the privacy and consumer protections under the CDR regime no matter who holds them – including data holders, accredited CDR participants and other third parties currently conceived under the umbrella term of non-accredited third parties.

This can be accomplished in a number of ways.

Extend strengthened Privacy safeguards to all consumers

Extending stronger privacy safeguards could be achieved by amending and strengthening the *Privacy Act* and the APPs to ensure that the same stronger protections under the CDR apply to all consumer data wherever it exists. We note that the ACCC and the Government have made some gestures towards implementing just this solution in the Government's response to the Digital Platform Inquiry including a review of the Privacy Act to

> *"…ensure it empowers consumers, protects their data and best serves the Australian economy. A review will identify any areas where consumer privacy protection can be improved, how to*

ensure our privacy regime operates effectively for all elements of the community and allows for innovation and growth of the digital economy

Introduce a new accreditation tier

The CDR can and should accommodate the use cases captured in response to Question 7 of this current consultation[42] by designing an accreditation system that appropriately extends the consumer protections of the CDR to these use cases and sets accreditation standards that appropriately reflect the different role played by potential entities who are currently considered non-accredited third parties, such as accountants, real estate agents etc. This may involve reduced requirements, but should include all the safety and security requirements that would ensure consumers remain protected. This submission addresses accreditation criteria in answer to questions 8 and 9 below.

Provide warnings

While not a solution, an option that must be considered is to include a warning to consumers to state that the protections under the CDR will not apply. We note that this is in fact the Maddocks' Privacy Impact Assessment Recommendation 3.2, that is to:

> *include an obligation on Data Holders to "warn" CDR Consumers when providing them with their CDR Data pursuant to their request (for example to state that the protections of the CDR regime (and possibly the APPs) will not apply if they provide that data to a third party). Similarly, if an Accredited Data Recipient discloses CDR Data to the CDR Consumer (which is a 'permitted use' of that CDR Data), indicate whether a similar protection is required in these circumstances;*[43]

We also note that the subsequent Agency Response puts forward two arguments against taking this action. Firstly:

> *The privacy risks associated with providing human readable data directly to the consumer is lower than the risks of providing machine readable data, being similar to the risks associated with consumers currently having an ability to view their own bank statements.*[44]

Subsequently the Agency Response states:

> *The suggested "warning" may unduly discourage consumers from accessing their data through the CDR regime in a situation where privacy implications are lower than for other methods of data sharing, such as screen scraping, for which no warnings would be required.*

---

[42] That is: "7. If the ACCC amends the rules to allow disclosure from accredited persons to non-accredited third parties and you intend to: a. receive CDR data as a non-accredited third party, please explain the goods or services you intend to provide, the purposes for which you propose to receive CDR data, and how this may benefit consumers; b. be an accredited person who discloses CDR data to non-accredited third parties, please explain the intended goods or services you intend to provide and how they may benefit consumers."

[43] Page 10, Maddocks, Department of the Treasury, Consumer Data Right Regime [Analysis as at 23 September 2019], PIA report finalised on 29 November 2019

[44] Page 8, Treasury, ACCC, OAIC, Data61, Consumer Data Right Privacy Impact Assessment Agency Response, December 20 9

We adamantly reject these arguments.

Firstly is not clear from this current consultation whether the disclosure of CDR data to non-accredited third parties would be done so in human readable format or machine readable format. Either way we maintain that protections for consumers must be provided.

With respect to the case where CDR data provided to non-accredited third parties would be restricted to human readable formats - all human readable material is currently machine readable anyway through scanning technology. Any Adobe PDF reader can do this right now and can be combined with screen scraping technology to extract the appropriate data. While this is more complex, it is still worth it for many entities to undertake this process.

With respect to the risk "being similar to the risks associated with consumers currently having an ability to view their own bank statements" again we point out that

a. the CDR produces higher volume, more detailed data, at greater speed; and
b. the CDR is meant to create a safer and more secure system to what currently exists.

With respect to warnings unduly discouraging consumers from accessing their data through the CDR – we reject that any warning here is undue. The risks are just as bad or worse as they are for existing forms of access, because of the higher volume, more detailed data that can be accessed at greater speed, - albeit through a slightly more complex extraction process as described above.

Even if it were to be conceded that the risks were lower, not providing a warning to consumers of the very real risks that exist would be a derogation of the duty of regulators of the CDR to keep consumer data safe at the same time as encouraging consumers to take part in the CDR. If the agencies overseeing the CDR choose not to provide a warning, then they take the real risk of fundamentally undermining consumer confidence in the CDR the first time a significant breach occurs.

We do note that warnings may not be sufficient to mitigate against the risks involved. Recent ASIC research found that:

> *There is emerging evidence from financial services regulators about the limitations of the effectiveness of warnings that firms have to display about the risks and features of certain products and services. … Warnings are not a cure-all for problems in financial services markets.*[45]

We agree with ASIC that warnings are insufficient and should not be seen to be as a solution. Nevertheless, warnings could play a minor role in preventing a small proportion people from engaging in risky behaviour.

Ban screen-scraping

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

If the delivery of CDR data to non-accredited parties is limited to human readable formats, another solution to prevent misuse of the data would to ban screen scraping – as the UK and EU have done.

We have outlined why screen-scraping must be banned alongside the introduction of the CDR regime in our recent submission to the Senate Select Committee on Financial Technology and Regulatory Technology's inquiry into Financial Technology and Regulatory Technology. We have attached the section detailing the full reasons why this is the case at **Attachment A**.

Recommendations

17. **No non-accredited third parties should be permitted to receive CDR data and that it is inappropriate for any unaccredited third party to receive and hold CDR data.**
18. **If it is decided that non-accredited third parties are permitted to receive CDR data then one of the following option must be implemented to ensure that the privacy and consumer protections of the CDR regime are extended to those consumers:**
    a) **Extend strengthened Privacy safeguards to all consumers;**
    b) **Introduce a new accreditation tier; and/or**
    c) **Provide warnings.**
19. **Screen-scraping should be banned.**

9. What privacy and consumer protections should apply where CDR data will be disclosed by an accredited person to a non-accredited third party?

As we have noted we do not support the concept of an accredited person being able to transfer CDR data to a non-accredited third party.

It is essential that *all* the strengthened privacy and consumer protections afforded consumers under the CDR regime should be extended to consumers whose data has been held, misused, abused, exploited or breached by a non-accredited third party. The same strong sanctions and remedy regime should also be applied to non-accredited third parties.

This means that the following Privacy Safeguards should apply and would substitute the APPs:

- Privacy Safeguard 1. Open and transparent management of CDR data
- Privacy Safeguard 2. Anonymity and pseudonymity
- Privacy Safeguard 6. Use or disclosure of CDR data
- Privacy Safeguard 7. Use or disclosure of CDR data for direct marketing by accredited data recipients and designated gateways
- Privacy Safeguard 8. Cross-border disclosure of CDR data
- Privacy Safeguard 9. Adoption or disclosure of government related identifiers

- Privacy Safeguard 10. Notifying of the disclosure of CDR data
- Privacy Safeguard 11. Quality of CDR data
- Privacy Safeguard 12 Security of CDR data; and
- Privacy Safeguard 13 Correction of CDR data

Non-accredited third parties should also meet the following as set out under the CDR Rules:

- Consent requirements
- Deletion and de-identification of CDR data rules
- Notification rules.

We also believe that non-accredited third parties should have the following in place:

- internal dispute resolution processes;
- be a member of a recognised external dispute resolution scheme;
- have addresses for service;
- have adequate insurance;
- establish a formal governance framework for managing information security risks relating to CDR data;
- have and maintain an information security capability
- meet minimum information security controls;
- have procedures and practices in place to detect, record, and respond to information security incidents as soon as practicable.

Recommendations

20. **All strengthened privacy and consumer protections provided to consumers under the CDR regime should be extended to consumers whose data has been held, misused, abused, exploited or breached by a non-accredited third party.**
21. **Non-accredited third parties should also meet CDR Rules appropriate to their role and should have appropriate administrative and procedural protections place to protect consumers.**

10. What degree of transparency for CDR consumers should be required where an accredited person discloses CDR data to a non-accredited third party? For example, are there particular consent and notification obligations that should apply?

Again, as we have noted we do not support the concept of an accredited person being able to transfer CDR data to a non-accredited third party.

If this were to nevertheless occur, it is essential that at the very least a warning is provided to the consumer who intends to act in this way. To not provide a warning would be to place consumers at serious risk.

Furthermore, we believe that the same consent and notification requirements that apply under the CDR rules should apply here. The reason for this is clear. The same safety and security issues arise when a non-accredited third party receives CDR data holds data as they arise with an accredited party.

Specifically consent must be given by a CDR consumer to a recipient to collect and use CDR data and that is:

(a) voluntary; and

(b) express; and

(c) informed; and

(d) specific as to purpose; and

(e) time limited; and

(f) easily withdrawn.[46]

Recipients of CDR data should meet the consent rules under the CDR Rules including:

- asking CDR consumer to give consent to collect and use CDR data, including the information they need to present to the CDR consumer when asking for consent: Rule 4.11;
- restrictions on seeking consent should be in line with the requirements: Rule 4.12.
- rules regarding the withdrawal of consent to collect and use CDR data and notification: Rule 4.13;
- limits on the duration of consent to collect and use CDR data: Rule 4.14;
- information relating to de-identification of CDR data: Rule 4.15
- rules regarding the election to delete redundant data: rules 4.16-4.17

We also believe that the notification requirements under Subdivision 4.3.5 should apply.

As mentioned above, recipients should also meet the rules with respect to the authorisation to disclose CDR data.

Whether non-accredited third parties should have to maintain consumer dashboards etc given they are not creating apps, is unclear but may depend on use cases presented.

[46] 4.9

Recommendations

22. **The same consent and notification requirements that apply under the CDR rules should apply to the passing of CDR to a "non-accredited Third Party."**

Appendix C:

Extract from the Joint Consumer Submission to the Senate Select Committee on Financial Technology and Regulatory Technology, December 2019.

Prohibit unfair trading practices

The Final Report of the Financial Services Royal Commission identified six norms of conduct, one of which was to 'act fairly'.[47] The norm of fairness is also recognised in the objective of the *Competition and Consumer Act 2010* (Cth) which is 'to enhance the welfare of Australians through the promotion of competition and *fair trading* and provision for consumer protection.'

Just as the concept of fairness must be applied in the "real world" financial services sector, the same must be applied to the FinTech sector.

Enacting an economy-wide prohibition on unfair trade practices as recommended by the ACCC in the Digital Platforms Inquiry will ensure fairer outcomes for consumer across the real world and digital economies.

This has been supported by Government who has backed the work of Consumer Affairs Australia and New Zealand on exploring how an unfair trading prohibition could be adopted in Australia to address potentially unfair business practices.[48]

Unfair business models and practices are incessant

Consumer harm continues in the face of existing consumer protections. Harmful business models and practices persist and case law confirms that practices that are unfair may not be unlawful. Harmful business models and practices that are not strictly unlawful have already begun to emerge in the FinTech sector and the digital environment more broadly. Some of these have been outline above with respect to screen scraping practices and issues with respect the application of AI but also include:

- Services requiring provision of detailed personal information without a business or legitimate reason for that information, enabling the service to monetise that information through profiling, target marketing or on-selling;
- Subscription traps, which include business models that are free upfront or for an initial period, but terms and conditions require ongoing payment[49]

[47] Royal Commission into Misconduct in the Banking, Finance and Superannuation Industry, Final Report, page 8.

[48] Regulating in the digital age Government Response and Implementation Roadmap for the Digital Platforms Inquiry, December 2019, https://treasury.gov.au/sites/default/files/2019-12/Government-Response-p2019-41708.pdf

[49] See, e.g., https://www.choice.com.au/shopping/online-shopping/buying-online/articles/beware-subscription-traps-warns-accc

- Services, memberships or marketing emails that make cancellation difficult, or employ deliberately confusing or tricky questions or processes to cancel.[50]
- Bundling products or services in such a way that prevents price comparison;[51]
- Charging loyal customers far more for the same product compared to new customers, without a legitimate justification or economic reason[52]
- Marketing practices or product disclosures that do not include clear, upfront and timely information that may lead the purchaser into error; and
- Business models that target consumer vulnerabilities or behavioural biases, distorting the consumer's free choice

The operation of the free market in Australia has failed to deliver fair outcomes for everyone. The above list demonstrates this—the market has not prevented these substantive unfair practices from becoming widespread. Moreover, these unfair practices are more likely to impact disadvantaged or vulnerable groups. Consumers that are less savvy or less able to protect their own interests, for example due to factors like age, language, health or capacity, are more likely to experience detriment associated with unfair practices.

It is sometimes suggested that more effective competition will incentivise suppliers to meet customer needs. Effective competition is indeed an important discipline on business conduct. However, there is a real risk that competition without appropriate legal and regulatory safeguards can fail to deliver fair outcomes.

The DPI Final Report confirms problems with competition in the context of digital platforms, and market power held by the large digital platforms such as Facebook and Google. However, it is highly unlikely that more competition will deliver fairer outcomes. As identified by the ACCC, harmful practices relating to data collection (including location tracking, online tracking for targeted advertising purposes, and the disclosure of data to third parties) are common in businesses beyond the big digital platforms. The business incentives created by competition and free market orthodoxy serve to embed these practices of concern, rather than deliver on community expectations relating to fairness. It is for this reason that consumer law has a very important role to play.

Conceiving fairness: the scope of a provision on unfairness

[50] See, e.g. Mathur et al, 'Dark Patterns at Scale: Findings from a Crawl of 11k Shopping Websites', July 2019, available at: https://webtransparency.cs.princeton.edu/dark-patterns/assets/dark-patterns-v2.pdf Page 15-16 includes a frustrating example: "Are you sure you want to cancel your membership" You will no longer receive membership pricing: click "continue" or "cancel". Another example involves consumers choosing the buy now, pay later option at an online check out with no way to go back, effectively locking the consumer into the transaction.

[51] See, e.g., https://www.darkpatterns.org/types-of-dark-pattern/price-comparison-prevention

[52] See, e.g., Competition and Markets Authority, Loyalty Penalty Super-Complaint, available at: https://www.gov.uk/cma-cases/loyalty-penalty-super-complaint

An economy-wide provision prohibiting unfair trade practices should ensure that not only the practices of firms are fair in terms of the processes followed but in terms of the outcomes delivered. This would include, for example, the prices consumers pay. This supports a move towards outcomes-based regulation and a focus on good culture within firms. Such an approach can also mitigate harms associated with unequal outcomes among different classes of consumers in market, particularly consumers experiencing vulnerability.

This can be achieved through a simple principles-based provision prohibiting unfair trade practices, including practices that are likely to have an unfair outcome. The detail of the provision can be left to guidance from regulators about expectations of firms, as well as later interpretation of the courts. In this way, a prohibition on unfair trade practices can complement the other principles-based provisions in the ACL. To operate as a community norm, in both a preventative and remedial fashion, we consider it unnecessary for the scope of the provision to be restricted or limited in the legislation itself.

That said, it is helpful to conceive the scope of such a provision to understand its import and impact. In conceiving the scope of a provision prohibiting unfair trade practices, we consider that it is helpful to consider the life course of a consumer transaction or service in the FinTech context: covering sales and marketing; product/service design & pricing; as well as service elements, including post-sale customer service. It is also useful to draw upon the analytical framework that already exists for unfair contract terms, that is, whether there is a legitimate business purpose associated with the particular practice and whether it results in an imbalanced outcome for the consumer.

Marketing: addressing manipulation

Marketing that impacts or restricts the freedom of choice of a consumer (without good reason) might be considered manipulation and an unfair trade practice. Manipulation also involves consumer harm that that is not reasonably avoidable by a consumer.

The widespread digitisation of commerce has given firms an enhanced ability, not only to compile detailed customer profiles, but also exploit consumers' cognitive biases and individual vulnerabilities. The collection of a greater amount of intimate and personalised data creates the opportunity to target market, and even subvert or manipulate reasonable decision-making by consumers.

A provision that enables consideration of the impact on the consumer (i.e. was, or is it likely, that harm is incurred) will improve the operation of consumer law; compared to unconscionable conduct which focuses on the conduct of the firm and whether it is against some sort of social norm.

Core product purpose: design and pricing

Clearly identifying a core product purpose is an important aspect of fairness, as it provides a yardstick for assessing consumer outcomes. A consumer product or service needs to have a reason for existing (other than a customer paying for and using it, and the firm supplying it).

A related aspect of fairness involves ensuring that the commercial returns to the firm associated with the product arise predominantly from consumer outcomes that are consistent with the product's purpose. This analysis would then help identify unfair practices—such as, offering discounts to new customers that aren't replicated for loyal/ongoing customers (a problem in insurance, mortgages, energy) or paying intermediaries (brokers, advertisers, comparison websites) rebates or commissions, creating risks associated with misaligned incentives.

This analysis builds on existing rules around fitness for purpose but has a greater focus on fair outcomes, that is, is the product or service likely to meet a consumer need. A key limitation of the existing ACL provisions relating to fitness for purpose is that the generally only apply if the consumer discloses their purpose for purchasing a particular product or service.[53] In most instances, consumers do not disclose a specific purpose.

Addressing vulnerability: universal design

Fairness is also about ensuring consumers experiencing vulnerability do not experience worse outcomes than more savvy consumers. Where consumers have limited ability to maximise their wellbeing, or have difficulty in obtaining or assimilating information, due for example to age, disability or background, they are less able to buy, choose, or access suitable products.

A requirement around fairness can require a better balance between business and customer responsibilities—it can help address the incessant problems caused by long and impenetrable terms and conditions by ensuring that businesses are more upfront with their customers. It can also require businesses to identify potential consumer harm caused by their products and service systems, adopting a 'prevention is better than cure' approach. Importantly, it can also address problems in the area of customer service and complaints processes, which can commonly benefit only those who are able to navigate the complexity rather than those who experience vulnerability. An unfair trade practice may be one that incorporates unnecessary barriers to service assistance.

Fairness can also help establish a universal approach to addressing vulnerability, moving away from a policy approach that focused solely on specific areas of disadvantage. In this way, a regulatory focus on fairness would improve the position of all consumers, including those who need more support due to their vulnerable characteristics or circumstances.

Recommendations

23. The Committee should endorse the development of an economy-wide prohibition on unfair trading practices, capturing FinTech practices.

[53] Sections 55 and 61, ACL.

Appendix D:

Extract from the Joint Consumer Submission to the Senate Select Committee on Financial Technology and Regulatory Technology, December 2019.

Develop a legally enforceable AI Ethical Framework

In order to support an appropriate regulatory regime for FinTech companies to achieve positive outcomes for consumers then the Committee must put ethical questions around technology, innovation and data front and centre of this consideration. This is particularly the case with respect to the use of Artificial Intelligence in FinTech.

Financial services and Artificial Intelligence

In the financial services sector new computing power and technology has led to:

- an expansion of the data collection from their own customers as well as from external sources both conventional (e.g. government databases and transactional data), and unconventional (e.g. social media, emails etc.);
- advanced data processing techniques; and
- advanced analytical, artificial intelligence and algorithmic techniques including predictive analytics.

AI is consequently well suited to exploitation in the financial services sector given AI's ability to recognise patterns, predictively anticipate future events based on large sets of data and make decisions based on this information. The example above of payday lenders hawking loans to individuals when it detects low bank balances is evidence of this.

The burgeoning FinTech sector is creating products, services and tools that are transforming ways the sector undertakes risk assessment, detects and manages fraud and assists consumer manage their finances.

New and emerging services involving some element of AI technologies include:

- new services embedded in mobile and online banking;
- Open Banking applications using consumer transaction data to assist in a series of services including but not limited to account switching, mortgage search services;
- new personal financial management services (such as Money Dashboard);
- investment and wealth management services with automated or robo-advisers services such as Wealthfront;
- new lending and unsecured credit services based on data led credit-scoring and risk profiling (e.g. Afterpay, Defer It);
- encrypted digital wallets that store bank, debit or credit card detailing for online payments (e.g. PayPal and AliPay);

- neo banks and FinTech savings banks such as AliPay's Yu'eBao;
- offline mobile payments such as Apple Pay, Android Pat or Ali Pay used at retail locations; and
- credit scoring and social scoring – utilising financial and social datasets from non-traditional sources such as Facebook and other social media to create measures of credit worthiness, outside of the "traditional" credit reporting and scoring.

There is also a sub-class of FinTech known as insurance technology or InsurTech. InsurTech is using AI technologies in three key ways.

Firstly it is using AI to build behaviour into premium pricing. Connected devices and telematics technology (e.g. Fitbit), connected home technologies (e.g. Amazon Alexa) and what is known as the "Internet of Things" (e.g. connected smoke alarms, locks, fridges and light switches) are also being put to specific use by the insurance sector.

Telematics technologies involve the use of GPS technology and increased information processing power to collected and transmit information and data to insurers directly. Telematics devices being used by insurers include:

- Motor vehicle telematics – devices in vehicles that can record GPS location data as well as information from a vehicle's engine management system to monitor all aspects of driving style. QBE, for example, offers "Insurance Box for young drivers". Here, drivers install an electronic device or "black box" in their car that transmits back to the insurer a detailed breakdown of their driving habits in areas such as their braking, acceleration, steering, cornering, speed and night driving.[54] QBE then calculate a "DriveScore" rating to evaluate the driver. The higher the DriveScore the less the policyholder will pay for insurance. The lower the score, the more the driver pays.
- Home telematics – devices can monitor the use and supply of a range of utilities as well as security of a home. Smart smoke alarms, water leak and freeze detectors are already being used overseas by insurers.
- Health monitors – fitness monitors such as Apple Watch and FitBit can record the location, movement, activities and other health information. AIA vitality[55] is an example of a product that enables a life insured to gain benefits such as discounts and rewards via the earning of "vitality points" for activities undertaken.[56] Others include Asteron Life Plus Health Rewards and Bupa Living Well.

Life insurers are using genetic testing technology in their underwriting provided to them under disclosure laws, an ability borne of increased computing processing power, new hardware and data analytics.

[54] https://www.qbe.com.au/news/car/how-insurance-box-works

[55] https://www.aiavitality.com.au

[56] https://www.aiavitality.com.au/vmp-au/rewards

AI is also being used in insurance to personalise the customer experience through the use of chatbots and other tools to improve the sales experience.

And finally AI is being used to 'enhance' the claims handling process including fraud detection through data analysis and machine learning, and speeding up the settling of claims. Many of the FinTech and InsurTech services are using algorithms and AI for automated decision making, sometimes with adverse outcomes.[57] Developing an enforceable AI ethical framework will assist in driving positive outcomes for consumers.

Ethical implications of the use of AI in financial services

FinTech products and services' utility arises from a near total reliance on data – largely a consumer's personal financial data - their transactions history, credit history, biometrics etc. FinTechs and InsurTechs are also integrating financial data with other data about individuals drawn from social media and other sources – information that people would consider have nothing to do with their financial status. InsurTech is tracking people's every movement and drawing conclusions about a person's identity and their life derived from the use of their car.

This increased collection of data is feeding the creation of a "financial identity" – a concept increasingly used by financial institutions to take user data and make assumptions based on that.

Financial institutions have for years stored and verified customer identities and attributes through "Know Your Customer" systems i.e. the process by which banks or other financial institutions identify their customers in order to evaluate the possible legal and other risks. They therefore have a commercial incentive to collect more and more accurate information about their individual customers. The World Economic Forum in 2016 has in fact argued that financial institutions "should champion efforts to build digital identity systems, driving the building and implementation of identity platforms."[58]

However the development of an increasingly accurate financial identity built by data has serious consequences for consumers.

Some positive impacts include enabling increased access to financial services and potentially empowering consumers in increasing their own financial literacy, behaviour or wellbeing.

There are however a series of impacts upon consumers – particularly consumers experiencing financial vulnerability or hardship - that are of significant concern to Financial Rights. We detail the following identified harms. While some of these cleave to ethical issues already raised in the Discussion Paper, there are new and further dimensions that we believe need to be considered in developing an Ethical Framework.

Profiling for profit: Increased economic inequality and financial exclusion

[57] For example, a media report in the UK claimed that drivers were charged significantly different amounts based on their name: https://www.newstatesman.com/politics/uk/2018/01/higher-insurance-if-you-re-called-mohammed-s-just-start-institutionalised

[58] World Economic Forum & Deloitte (2016) "A Blueprint for Digital Identity: The Role of Financial Institutions in Building Digital Identity": page 28
http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

Financial Rights is concerned that with the rise of AI in FinTech, we will see increased occurrences of consumers being 'profiled for profit', which will see more people experiencing financial difficulties being offered unsuitable (but highly profitable) products. Or excluded

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

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

We have seen other highly risky and harmful 'Fintechs' such as contracts-for-difference providers engage in regulatory arbitrage in the past, where Australia has been seen as a soft target and used as a regulatory base for predatory investment platforms.[59]

What is of more significant concern is that with the automating of these processes through an Open Banking regime and the application of AI to this, there will be significant room for increased exploitation. Consumer advocates in the United Kingdom, have already raised concerns that 'Open Banking enables lenders to continually monitor accounts and take repayment as soon as income is detected'[60]. These are real risks that are poorly understood by consumers and unlikely to be dealt with by disclosure and consent because of the take it or leave nature of the service.

Price discrimination on low-income households

Much of the promise of FinTech is that more tailored products and services will be made available with lower fees or lower loan interest rates for many banking customers. However, the flip side to lower fees and interest rates for some is that costs will increase for others. These 'others' will undoubtedly be Australia's most vulnerable, disadvantaged and financially stressed households.

Those in more precarious financial situations – again identified as such by their data driven financial identities - will likely be unfairly charged higher amounts for credit, or be pushed to second-tier and high cost fringe lenders. In other words, the consumers who can afford it the least will pay the most be it via higher interest rates or higher fee products. There are serious fairness considerations at play here. As banks and credit providers are increasingly able to use consumer data and technology to better automate the targeting of particular financial services

[59] Australian Financial Review, *CFD players accused of 'regulatory arbitrage'*, 22 August 2019, https://www.afr.com/companies/financial-services/asic-to-ban-retail-2b-in-risky-derivatives-20190822-p52jkt

[60] Open Banking, A Consumer Perspective, Faith Reynolds, January 2017 http://docplayer.net/39177571-Open-banking-a-consumer-perspective-faith-reynolds.html

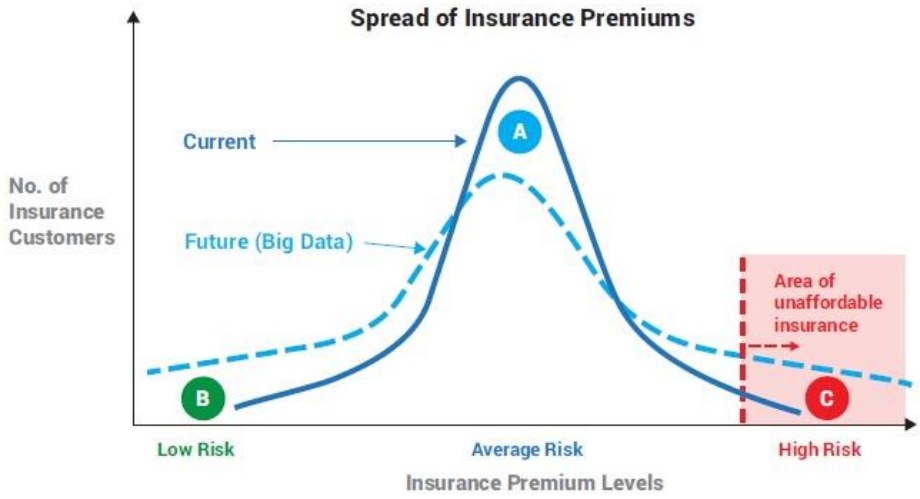
offers to profitable' consumers, we will likely see an increased use of 'risk-based pricing'. This may result in some lenders targeting 'riskier' borrowers with higher interest rates. While risk based pricing has effectively existed in Australia in the non-bank sector for some years, it is now moving into mainstream banking.

A 2015 report by United States organisation Data Justice raised concerns that enabling advertisers to offer goods at different prices to different people to extract the maximum price from each individual consumer. The report found that such price discrimination not only raised prices overall for consumers, but particularly hurts low-income and less technologically savvy households.[61] In fact, the ability to segment the market further will likely mean that firms can 'cherry pick' the most commercially viable consumers and exclude others (or charge them more).[62]

It is clear that the result of the price discrimination in credit enabled by these technologies in the financial services sector is a downward spiral of debt. A self-fulfilling prophecy ensues. A consumer's low credit rating decreases from a default, which in turn feeds an algorithm of credit-worthiness leading to higher interest rates and further financial difficulty and further defaults.

In the insurance sector, the increased use of big data analysis and automated processing allowed by increased computing power will enable insurers to increasingly distinguish between risks on an increasingly granular level. This will lead to the higher risks only being able to be insured for higher prices or on worse terms. According to the Actuaries Institute

> *At the extreme, some policyholders will have their risks assessed as so high that the price will be prohibitive or insurers will decline to provide cover. The following diagram illustrates the effect that increasing data will have on insurance premiums.*



[61] Data Justice, Data Justice Report: Taking on Big Data as an Economic Justice Issue, 2 October 2015, available at: http://www.datajustice.org/blog/data-justice-report-taking-big-data-economic-justice-issue

[62] 7 Faith Reynolds, Open Banking: A Consumer Perspective, January 2017, p. 23, available at: https://home.barclays/content/dam/home-barclays/documents/citizenship/access-to-financial-and-digital-empowerment/Open-Banking-A-Consumer-Perspective-Faith-Reynolds.pdf

Overall, there will be fewer insureds treated as "average" risk (area A) and paying average premiums. They will increasingly be classed as either lower or higher than average. Greater numbers of insureds will thus be recognised as being lower risk and given lower insurance premiums (area B). Conversely there will be more consumers falling into the higher risk category, ultimately reaching the "unaffordable" levels of insurance premiums (area C).

…

In response, some people may mitigate or avoid the risk. Others who find the insurance premiums for their risk to be unaffordable may have to take the risk themselves. If the risk event does happen, they will suffer financially. The more people change from insured to uninsured status because of price increases arising from more targeted use of data, the greater the burden will be on the public purse or on others outside the insurance system.[63]

Unfair and exclusionary price discrimination practices in insurance and the broader financial services sector should be a cause for serious concern where it contributes to lower-income people paying higher prices than others, or where pricing discrimination negatively affects particularly marginalised groups. In the insurance sector, people who need insurance the most may increasingly find they have been excluded completely as a result of issues which may be completely beyond their control. These are key issues of fairness and equity which this Committee should consider and address. Such exclusion also flies in the face of government efforts to increase financial resilience, and ultimately puts pressure back on the government and community to pick up the pieces where the market has failed and those affected are in no position to cover their own losses.

Indirect Discrimination

Algorithmic decision making in the financial services sector has great potential to introduce bias into decision making particularly for marginalised consumers.

Researchers have pointed to a "system in which power over the judicious and ethical use of data is overwhelmingly concentrated among white men" resulting in negative consequences for minority groups.[64] This is because unconscious biases that are held by an individual or group of individuals becomes part of the technology that they create. Questions around what data should be collected, how it is used and who is making these decisions need to be interrogated.

Closed proprietary algorithms used by FinTechs and InsurTechs to automatically calculate an individual's credit worthiness or the interest rate they are offered could also potentially lead to situations where consumers are denied access to crucial products and services based on accurate or inaccurate data without the ability to determine why or to correct underlying assumptions.

[63] Page 19-20, Actuaries Institute, The Impact of Big Data on the Future of Insurance https://actuaries.asn.au/Library/Opinion/2016/BIGDATAGPWEB.pdf

[64] https://theconversation.com/data-ethics-is-more-than-just-what-we-do-with-data-its-also-about-whos-doing-it-98010

Algorithmic bias or discrimination is already well documented[65] and arises when an algorithm used in a piece of technology – say a FinTech product or service – that reflects the implicit or explicit values of those who are involved in coding, collecting, selecting, or using data to establish and develop an algorithm.

Credit scoring, social scoring or e-scoring algorithms for example can produce feedback loops where somebody from a particular suburb where a lot of people default can be given lower credit ratings due to that association, or where a particular address is charged a higher premium based on the habits and attributes of previous occupants – an example that a client of Financial Rights experienced. Statistical correlations used by actuaries between a person's postcode (here geographical information standing in for a particular race, ethnicity or culture); their language patterns on social media; their potential to pay back a loan; or, keep a job; can lead to significant discrimination being built into opaque black box algorithm technology.

Cybercrime, identity theft and material theft

As our financial services sector becomes more and more reliant on technology with greater access to accurate personal information– the fuel on which AI depends – individuals become increasingly vulnerable to cybercrime.

Firstly consumers are vulnerable to identity theft. With increasingly sensitive and accurate data being held by FinTechs, breaches of these datasets make it easier for criminals to use this identifying information to undertake subsequent crimes, financial or otherwise.

The vulnerability of the data protection systems in place also facilitates actual theft of property – that is the hacking of FinTech systems to access payment systems and steal money. According to Juniper Research, fraudulent online transactions will reach a value of $25.6 billion by 2020[66] In Australia online credit card fraud, with transactions made using stolen card details hitting $417.6 million in 2016, more than doubling since 2011.[67]

The news[68] 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 in various ways. Combined with the never-ending list of significant and high profile data breaches at Equifax, Ashley Madison, Yahoo and more, consumer awareness of how vulnerable consumers are is increasing every day.

A legally enforceable AI Ethics Framework is required

---

[65] See Cathy O'Neil, Weapons of Math Destruction, 2017

[66] "Online Transaction Fraud to More than Double to $25BN by 2020' Juniper Research UK, May 2016.

[67] Lucy Cormack, Carol Saffer, Online credit card fraud on the rise, accounting for 78 per cent of total card fraud in Australia, SMH, 3 August 2017 https://www.smh.com.au/business/consumer-affairs/online-credit-card-fraud-on-the-rise-accounting-for-78-per-cent-of-total-card-fraud-in-australia-20170802-gxnwd7.html

[68] 'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower, *The Guardian*,18 March 2018 https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump

This Inquiry presents an opportunity to help embed principles within the FinTech sector that ensure they promote ethical value creation rather that value appropriation.

The Department of Industry, Innovation and Science recently developed a set of voluntary principles that are designed to be used when designing, developing, integrating or using artificial intelligence (AI) systems.[69]

The eight principles are:

- *Human, social and environmental wellbeing: Throughout their lifecycle, AI systems should benefit individuals, society and the environment.*
- *Human-centred values: Throughout their lifecycle, AI systems should respect human rights, diversity, and the autonomy of individuals.*
- *Fairness: Throughout their lifecycle, AI systems should be inclusive and accessible, and should not involve or result in unfair discrimination against individuals, communities or groups.*
- *Privacy protection and security: Throughout their lifecycle, AI systems should respect and uphold privacy rights and data protection, and ensure the security of data.*
- *Reliability and safety: Throughout their lifecycle, AI systems should reliably operate in accordance with their intended purpose.*
- *Transparency and explainability: There should be transparency and responsible disclosure to ensure people know when they are being significantly impacted by an AI system, and can find out when an AI system is engaging with them.*
- *Contestability: When an AI system significantly impacts a person, community, group or environment, there should be a timely process to allow people to challenge the use or output of the AI system.*
- *Accountability: Those responsible for the different phases of the AI system lifecycle should be identifiable and accountable for the outcomes of the AI systems, and human oversight of AI systems should be enabled.*

The principles complement existing AI related regulations and are intended to:

- achieve better outcomes
- reduce the risk of negative impact
- encourage the highest standards of ethical business and good governance.[70]

While the establishment of this voluntary framework is a good start it is clear that this will not be enough moving into the future. As the AHRC recently stated:

[69] https://www.industry.gov.au/data-and-publications/building-australias-artificial-intelligence-capability/ai-ethics-framework/ai-ethics-principles

[70] https://www.industry.gov.au/data-and-publications/building-australias-artificial-intelligence-capability/ai-ethics-framework/ai-ethics-principles

> *The Australian Government's AI Ethics Framework, outlined above, is an important, but modest, step that aims to prevent social harm associated with AI.*[71]

The voluntariness of the ethics framework means that there will be:

> *no rigorous, independent way of holding an individual or corporation to account in adhering to these principles, and no concrete consequences that flow from a failure to adhere. This is not inherently problematic. A voluntary commitment to abide by certain ethical principles can influence behaviour. A problem arises, however, if such voluntary commitments occupy the proper place of enforceable legal rules.*[72]

The AHRC has subsequently recommended that the government begin the process of moving towards the reification of ethical frameworks into the law.

> *Ethical frameworks can be important, but they cannot be a substitute for the law. This is as true amid the rise of new technologies, as it is in any other context. The Commission considers that there is a need to re-articulate the conventional relationship between the law and ethics in regulating behaviour.*[73]

The AHRC consequently propose that:

> *The Australian Government should commission an appropriate independent body to inquire into ethical frameworks for new and emerging technologies to:*
>
> *(a) assess the efficacy of existing ethical frameworks in protecting and promoting human rights*
>
> *(b) identify opportunities to improve the operation of ethical frameworks, such as through consolidation or harmonisation of similar frameworks, and by giving special legal status to ethical frameworks that meet certain criteria.*[74]

We agree that this would be an important first step.

Australia has the potential to foster a growing, high quality and consumer focussed Fintech industry -setting high minimum standards would provide a strong foundation. It would also prevent a regulatory 'race to the bottom' and a culture that seeks to undermine regulators or exploit loopholes.

We also believe that the FinTech sector could act now and agree to adhere to the AI Ethics Framework via a Code of Practice. Alternative the ACCC CDR Rules should be amended to require CDR participants to meet these standards.

---

[71] Page 52, AHRC, Human Rights and Technology Discussion Paper https://tech.humanrights.gov.au/sites/default/files/2019-12/TechRights2019_DiscussionPaper.pdf

[72] Page 54, AHRC, Human Rights and Technology Discussion Paper https://tech.humanrights.gov.au/sites/default/files/2019-12/TechRights2019_DiscussionPaper.pdf

[73] Page 55, AHRC, Human Rights and Technology Discussion Paper https://tech.humanrights.gov.au/sites/default/files/2019-12/TechRights2019_DiscussionPaper.pdf

[74] Proposal 2, Page 57, HRC, Human Rights and Technology Discussion Paper https://tech.humanrights.gov.au/sites/default/files/2019-12/TechRights2019_DiscussionPaper.pdf