Australian Privacy Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

ACCC

By email: CDR-ACCC@accc.gov.au

Consumer Data Right – Consultation on how best to facilitate participation of third party service providers

This submission from the Australian Privacy Foundation (APF) responds to the ACCC Consultation Paper: *Consumer Data Right – consultation on how best to facilitate participation of third party service providers.*

General comments

The APF does not support the expansion of the rules to permit disclosure of Consumer Data Right (CDR) data from accredited persons to non-accredited third parties. We believe that including non-accredited third parties presents a significant risk of harm for consumers.

We remain concerned that there are significant risks (including privacy risks) for people using the CDR and we do not believe the CDR as drafted has sufficient consumer protection safeguards in place to enable its safe use. The proposed expansions in the Consultation Paper increase the risks of consumer harm.

Open banking must be a closed system

People need to be sure that when they use the CDR that all participants are fully accredited and a member of an external dispute resolution scheme (EDR). Any inclusion of non-accredited parties

presents a risk for consumers using the system. From a privacy perspective, non-accredited parties could cause the following harms:

1. People will not be able to easily follow the trail of their data. This is effectively a loss of control over their personal information which is inconsistent (and would be a breach) of the person's privacy.
2. The likelihood of a data breach would increase as security is likely to be poorer with small firms.
3. Consumers will not know how to complain or where as this may not be clear

Consumers must be confident that any party they deal with must be fully accredited, easily found and a member of an EDR.

Big problem 1: The data is more valuable than providing a service

A significant problem with open banking is that the personal information being obtained from a bank (at this first stage, it is a bank) is significantly more valuable than providing a service to assist people with for example, finding a better deal. This means that the provider is not incentivised to provide the service offered but are instead incentivised to collect the data. This leads to at least a potential if not actual conflict of interest.

The personal information held by banks is extremely rich and valuable. The ACCC has recently issued a Final Report on Customer Loyalty Schemes.[1] It states:

> *Consumer data is of significant value to loyalty schemes. The collection and analysis of consumer data is a key function of loyalty schemes. The rich data loyalty schemes collect about consumers includes their demographic data, transaction history, interests, preferences, consumption patterns, buying behaviour and habits.*[2]

It is reasonable to assume that the insights about rich personal information about customer loyalty schemes **will** apply for open banking. In fact, failing to plan to deal with these issues would be an obvious planning failure.

When the data is the main objective of the transaction (not the service being advertised/offered) then it is likely that the following harms will occur:

- Misuse of the data and other breaches of privacy;

[1] ACCC, Customer Loyalty Schemes Final Report December 2019.
[2] ACCC, Customer Loyalty Schemes Final Report December 2019, page 45

- Data breaches;
- Monetisation of consumer data;
- Profiling and targeting of consumers for poor value products and services;
- Discrimination and exclusion may ensue from data analysis;
- Increasing lack of trust in service providers using the CDR;
- Blaming banks for providing the data or other harms from the intermediary who induced them to change their banking; and
- Exposure to scams and rip-offs.

Interestingly, many of these possible harms are similar to the list provided by the ACCC in relation to potential harms with customer loyalty schemes.

The APF remains concerned that the CDR Rules do not adequately address the value of the data issue outlined above. Our numerous submissions have previously outlined many problems with the CDR legislation. We remain concerned that there will be widespread consumer harm because of this problem and it will be necessary to revise the CDR Rules to address these problems. At a minimum, the ACCC must:

- Limit access to only fully accredited organisations;
- Prohibit data transfers between accredited organisations;
- Provide a clear right in the CDR Rules to delete personal information;
- Closely monitor and audit data use; and
- Carefully monitor consumer outcomes.

Big problem 2: Data security and data breaches

Banks not only have obligations under the Privacy Act but also have a common law duty of confidentiality. They also have significant reputational concern and attention to security. All of these factors mean that data is far safer from misuse in a bank. Transfer of the data to a smaller organisation raises security concerns and data breach risks. Data breaches are common. It is a matter of "when" not "if". Data breaches currently require notification (but only if the breach is likely to result in serious harm to an individual personally involved)[3] but do not necessarily (and usually do not) lead to compensation.

It remains a problem that the consequences for a data breach remain between minimal and no consequence at all. For example, the OAIC has yet to take any action on the serious privacy breaches

[3] See OAIC About the Notifiable Data Breaches scheme at https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme/.

by Facebook when other Countries had enforced outcomes months ago. When the main incentive for providing a service is to get the valuable personal information and there are no consequences for data breaches this necessarily incentivises misconduct.

Big problem 3: Intermediaries

The CDR is a misnomer. Consumer's have had a right to access their own personal information held by another entity (regulated under the Privacy Act) since 1988. Consumers also have a range of other rights to access their own data (for example, under the National Consumer Credit Protection Act). Banks have been providing that data on request for many years (and even have a commitment to do so under the Banking Code of Practice). The difference with the CDR is that it transfers personal information to a third party that then provides some sort of service based on that personal information. Of course, the intention of this legislation is that this third party will provide a suitable and valuable service. The APF remains concerned that the third party will instead covet the personal information and put the consumer in a worse position.

There is a long history of consumer harm in Australia with the use of intermediaries. The Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry (Financial Services Royal Commission) found repeated systemic issues with intermediaries in its Final Report.[4] Several serious and systemic problems were identified with intermediaries in financial services that included:

- Difficulty working out who the intermediary acts for;
- The duties and responsibilities of the intermediary;
- Who the intermediary owes a duty and responsibility to;
- Problems with conflicted remuneration which influences advice and product choices; and
- The culture of intermediaries on managing risk.[5]

The Financial Services Royal Commission Final Report concentrated on the role of mortgage brokers and financial advisers. However, it was observed that these concerns do arise with a range of intermediaries (the example given in the Final Report was the use of intermediaries in car yards). Although, there have been some moves by the Government to implement recommendations from the Financial Services Royal Commission to resolve problems with intermediaries (for example a best interest duty for mortgage brokers), the Government will not be taking action on mortgage brokers and conflicted remuneration (as recommended in the Final Report).[6]

[4] Final Reports available at https://financialservices.royalcommission.gov.au/Pages/reports.aspx.
[5] For a summary see Financial Services Royal Commission Final Report Volume 1 pages 14 and 15.
[6] Recommendation 1.3 of the Financial Services Royal Commission Final Report. Government response: Restoring Trust in Australia's financial system see page 7 where the Government did agree to take action on trail commissions but took no action on the recommendation that the borrower should pay the mortgage broker not the lender.

In summary, this means that when consumers deal with intermediaries there is a demonstrated history of harm and more importantly, it is still unclear whether there are sufficient consumer protections in place to prevent future harm from licenced financial service provider intermediaries.

The Financial Services Royal Commission had a limited remit and there are a range of intermediaries that were not covered but do have a history of harm for consumers. Those intermediaries include:

- Finance brokers – these are intermediaries who arrange a loan that is not to buy or refinance real estate. They can arrange car loans, personal loans, credit cards, equipment finance, business loans etc. Finance brokers are poorly regulated, can be very expensive and arrange very unsuitable expensive loans.
- Debt Management Firms. Also called debt vultures. These firms are poorly regulated and provide services around budgets, negotiating with creditors, arranging Part IX Debt Agreements and credit repair. Many debt management firms offer multiple services. ASIC in Report 465 – Paying to get out of debt or clear your record: The promise of debt management firms[7] found significant problems with debt management firms.
- Solicitors and accountants being involved in predatory practices[8].

It is in the above context that the APF argues that significant consumer protections are required for consumers dealing with intermediaries. The current protections are inadequate.

In answer to the consultation questions (noting that we have already stated that the current protections are inadequate):

1. Intermediaries must comply with full accreditation standards under an accreditation model.
2. The obligations for intermediaries must be the same as any accredited data holder or data recipient.
3. As stated above, there is no way for consumers to reasonably keep track of who the intermediaries are even with disclosure (which will not work). The answer is to limit who can participate based on a range of criteria with consumer protection safeguards.
4. Data must not be transferred between accredited persons. If a transfer is required it must go back to the consumer owner of the data.
5. There must not be lower tiers of accreditation. Direct liability must be preserved at all times.

[7] Report released in January 2016. Available at https://asic.gov.au/regulatory-resources/find-a-document/reports/rep-465-paying-to-get-out-of-debt-or-clear-your-record-the-promise-of-debt-management-firms/.
[8] For example, see the role of accountants in predatory lending in ASIC Report 119 Protecting wealth in the family home: An examination of refinancing in response to mortgage stress March 2008 available at https://download.asic.gov.au/media/1344842/REP_119_Protecting_wealth_in_family_home.pdf.

Non-accredited third parties

Disclosure to non-accredited third parties must not be permitted.

If you have any questions please do not hesitate to contact Kat Lane.

Yours sincerely

Kat Lane,
Vice-Chair
Australian Privacy Foundation
0447 620 694
kat.lane@privacy.org.au

About the Australian Privacy Foundation

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions. The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems.

The APF makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters. Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance. When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.