Financial Rights LEGAL CENTRE

consumer action law centre

Joint submission by the
Financial Rights Legal Centre and
Consumer Action Legal Centre

Treasury

Open Banking: customers, choice, convenience, confidence, December 2017

March 2018

About the Financial Rights Legal Centre

The Financial Rights Legal Centre is a community legal centre that specialises in helping consumer's understand and enforce their financial rights, especially low income and otherwise marginalised or vulnerable consumers. We provide free and independent financial counselling, legal advice and representation to individuals about a broad range of financial issues. Financial Rights operates the National Debt Helpline, which helps NSW consumers experiencing financial difficulties. We also operate the Insurance Law Service which provides advice nationally to consumers about insurance claims and debts to insurance companies. Financial Rights took close to 25,000 calls for advice or assistance during the 2016/2017 financial year.

About Consumer Action Law Centre

Consumer Action is an independent, not-for-profit, campaign-focused casework and policy organisation. Consumer Action offers free legal advice, pursues consumer litigation and provides financial counselling to vulnerable and disadvantaged consumers across Victoria. Consumer Action is also a nationally-recognised and influential policy and research body, pursuing a law reform agenda across a range of important consumer issues at a governmental level, in the media, and in the community directly.

Introduction

Thank you for the opportunity to comment on the Open Banking Final Report. Consumer Representatives will address the key aspects of the proposed framework as it applies to consumers and the improved, or in some cases deteriorated, outcomes, that arise from the current recommendations.

We write this submission at a moment in time where data privacy and security issues are on the world's front pages and consumer awareness over the collection, use and potential abuse of personal data is growing exponentially.

For the past two decades, consumers have experienced the innumerable benefits of new technology, innovation and data with the commensurate positive impact on their private, social, financial and working lives. The speed of these changes has been bewildering, so it is only now that consumer understanding of the full impact of these changes is dawning on them with a growing awareness of the true down-side of digital innovation. From world-wide data breaches and increased direct marketing and targeting, to the rise of price discrimination, the segmentation of populations and even the potential undermining of the political process, consumers are beginning to more fully understand the implications of what they have signed up for.

Consumers are therefore entering into the Open Banking regime with a mix of expectation and wariness. In the development of the Open Banking regime and introduction of Consumer Data Right consumers see, on one side, banks and existing data holders who wishing to hold on to what is seen the gold mine of the future: our personal data. On the other side we have a FinTech sector who are keen to mine this ore for riches, presenting the innovations they produce as the solutions for many of the ills the financial sector is currently displaying, most prominently in the current Financial Services Royal Commission.

For consumers, there are many opportunities for improved outcomes, for bank switching and a vast array of new innovative financial services some they have been yearning for years, others that they don't even know they need. Development of the Open Banking regime and the Consumer Data Right also provides a once in a generation opportunity to fix issues with consent, and the unbundling of reams of unread terms and conditions.

However there are a number of potential issues with Open Banking that Consumer Representatives have already detailed in past submission to the review.[1] These include increased complexity and choice; increased economic inequality and financial exclusion, increased information asymmetry and predatory marketing and a large number of basic concerns with respect to privacy, security, unconscionable practices, the impact of non-transparent black box technology, flawed correction processes and more.

[1] Consumer Action, Financial Rights and Choice submission and supplementary submission found here: https://static.treasury.gov.au/uploads/sites/1/2017/09/c2017-t224510_CALC.pdf and https://static.treasury.gov.au/uploads/sites/1/2017/11/c2017-t224510-CALC-FRLC-FCA.pdf

Australia is coming late to the consumer data right party. The EU have taken strong strides into bolstering consumer protections in this space with the new General Data Protection Regulation (**GDPR**) from May 2018 and the Payment Services Directive 2 (**PDS2**) coming into force early this year in January 2018.

Australia does not have to re-invent the wheel and can learn from the lessons hard fought overseas and should follow the EU's lead or find itself out of step with international practice to the detriment of Australian innovators as well as Australian consumers.

The Report puts forward four straightforward principles for Open Banking:

- *Open Banking should be customer focussed. It should be for the customer, be about the customer, and be seen from the customer's perspective.*
- *Open Banking should encourage competition. It should be done to increase competition for the banking products and services available to customers so that customers can make better choices.*
- *Open Banking should create opportunities. It should provide a framework on which new ideas and business can emerge and grow, establishing a vibrant and creative data industry.*
- *Open Banking should be efficient and fair. It should be effected with security and privacy in mind, so that it is sustainable and fair, without being more complex or costly than needed.*

Consumer Representatives believe these principles are appropriate. We do wish to see innovation in the financial services sector to drive improved outcomes, however this will need to be balanced by genuinely effective consumer protections and access to justice. We strongly support the Report's placing of the customer at the centre of the regime. Our submission is drafted to ensure that the Report's final recommendations reflect this promise.

To live up to these principles placing the consumer interest at the heart of the Open Banking regime, the Report must recommend the following:

- the development of a full Consumer Right that includes the right to deletion (or erasure), without which the stated intention of the Report will fail;
- a thoroughgoing review and modernising of the *Privacy Act 1988* and the outdated and weak Australian Privacy Principles to provide improved safeguards for consumers and greater customer control over their data;
- a radical re-think of consent in the age of data;
- an accreditation scheme that ensures Open Banking entities meet appropriately high standards;

- regulatory oversight by the ACCC, ASIC, a reformed OAIC and genuine access to justice via the Australian Financial Complaints Authority as the central point for all complaints including those related to privacy and security concerns;
- greater transparency rights for consumers with respect to the uses of their data be it personal, transaction, value added or aggregated data – this is important for a removing asymmetry of information and providing a more ideal environment for a truly competitive market; and
- a ban on the practice of screen-scraping to prevent ongoing exploitation of vulnerable consumers.

Recommendations

Chapter 2: Open Banking Regulatory Framework

Recommendation 2.1 – a layered regulatory approach

1. **Consumer Representatives support Recommendation 2.1's layered regulatory approach.**
2. **A right to erasure should be included in the general Consumer Data Right empowering individuals to request the erasure of any links to, copy or replication of the data in question, where:**
    a) **the data is no longer necessary in relation to the purposes for which it was collected;**
    b) **the individual withdraws consent or the relevant storage period has expired;**
    c) **the individual objects to the processing of data; or**
    d) **the data was unlawfully processed;**
    e) **there is a legal requirement for the data to be erased; or**
    f) **the consumer is a child at the time of the collection.**
3. **Consumer groups must be a part of the rule and standard setting process and should be appropriately resourced to do so.**

Recommendation 2.2 – the regulator model

4. **The ACCC should act as the lead regulator in a government led, multiple regulator model which include ASIC, AFCA and the OAIC to administer and enforce the expansive Consumer Data Right.**
5. **The AFCA should be the central point for receiving complaints with respect to privacy breaches and all other issues with respect to the Open Banking aspect of the Consumer Data Right. It should be able to receive, investigate, facilitate the resolution of, make decisions and recommendations for, and report on, complaints about acts or practices of their members that may be an interference with the privacy of an individual.**
6. **The accreditation criteria should include provisions to ensure membership of the AFCA be compulsory for all companies.**

Recommendation 2.3 – the banking Consumer Data Right

7. **The sector by sector approach to implement a Consumer Data Right is appropriate as is the choice to have Open Banking be the first designated sector.**

Recommendation 2.8 – the accreditation criteria

8. **Consumer representatives are not opposed to a tiered accreditation regime however there must be baseline accreditation criteria that all tiers must adhere including:**

    a) **meeting privacy standards and security standards (as described in Chapter 4 of the Report) including a description of the process in place to file, monitor, track and restrict access to consumer data;**

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

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

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

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

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

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

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

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

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

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

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

9. **The sale of this data to fourth parties needs to be regulated and overseen under the Open Banking regime. We would prefer the practice be banned**

10. **The concept of sensitive information, as defined under the *Privacy Act* needs to be re-considered to ensure that financial information is appropriately protected.**

Recommendation 2.9 Responsibility for the address book

11. **A public address book or white list should be made available and maintained by the ACCC. For the purposes of public education, an accreditation logo or tick should be considered for inclusion on all accredited products or services.**

Recommendation 2.10 – Customer complaints and remedies

12. **A standardised, IDR process for *all* accredited open banking parties, big or small must be mandated and should meet best practice as outlined in *ASIC's Regulatory Guide 165: Internal and External Dispute Resolution*.**

13. **A one stop EDR framework based on the ombudsman model is essential for consumers to have access to justice. This should be AFCA. We agree with the Report that there should be "no wrong door" for consumers.**

Enforcement

14. **A strong and wide-ranging research, investigation and enforcement regime should be included in the Open Banking regime, with ACCC empowered with an expansive regulatory tool-kit.**

15. **There should be significant penalties and remedies for breaches to the Consumer Data Right and the Open Banking regime, as per the *Competition and Consumer Act 2010*.**

Chapter 3 – The scope of Open Banking

Recommendation 3.1 – customer-provided data

16. **Consumer representatives support recommendation 3.1.**

Recommendation 3.2 – transaction data

17. **Consumer representatives support recommendation 3.2 but may wish to consider new forms of credit and debit-like accounts that are developing such as By Now Pay Later platforms.**

Recommendation 3.3 – value-added data

18. **Consumer representatives do not support value-added data being included in the scope of the Open Banking regime.**

19. **Value-added data should be shared with the consumer for the sake of transparency. Consumers should have access to the types of insights that a data holder is creating and for what purposes they are using this data.**

Recommendation 3.5 – aggregated data

20. **Aggregated data sets should not be included in the scope of Open Banking.**

21. **Consumers should be able to withdraw consent for the use of aggregated data sets by a data-holder (or recipient) and that this data be destroyed.**

22. **The concepts of anonymised data (where re-identification is impossible by any party by any means) and pseudonymous data (except re-identification techniques are reasonably**

likely to be used) as per the GPDR should be embedded in the Consumer Data Right and the Open Banking regime.

23. Consumers should be fully informed and provide express consent to all uses of aggregated datasets (de-identified or otherwise), including who has access to them.

Recommendation 3.7 – application to accounts

24. Consumer representatives support recommendation 3.7 but recommend a consideration of the impact of Open Banking services on young people. , including restrictions similar to Article 8 of the GPDR.

Recommendation 3.11 – no charge for customer data transfers

25. Consumer representatives support recommendation 3.11 that there be no charge for customer data transfers.

Chapter 4 – Safeguards to inspire confidence

Recommendation 4.1 – application of the Privacy Act

26. Consumer representatives support recommendation 4.1 that all data recipients be subject to the *Privacy Act 1988*.

Recommendation 4.2 – modifications to privacy protections

27. APP3 must be updated and amended to ensure that an entity must not collect personal information unless the entity can demonstrate that express consent has been received from the customer which is:

    a) explicit;

    b) discrete for every use, purpose or function – that is, not bundled in any form

    c) fully informed;

    d) able to be permitted or constrained according to the customer's instructions including easily withdrawn with immediate effect.

    e) time limited.

28. APP3 must also ensure that data recipients explain in simple, clear, terms why information is being collected and for what it is being used. Data recipients must also be obliged to only collect the minimum of personal information that the business actually needs.

29. APP3 must also make clear that the lack of consent should not limit the ability to receive the service unless the data is necessary to the working of the product or service.

30. **APP4 must be amended to ensure that a data recipient who has received unsolicited banking data will need to either gain express consent or be required to destroy or de-identify the unsolicited personal information.**

31. **APP5 must be modernized to require notifications to be made, acknowledged and recorded.**

32. **APP6 must be updated to ensure that a data recipient should demonstrate that any secondary use is directly related to the primary purpose.**

33. **APP7 should be updated to require customers provide their express consent before a data recipient can directly market to the customer. This should not be bundled with other consents.**

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

35. **The on-sale of personal data provided to the data recipient and created by the data recipient through the customer's use of the product or service should be covered by similar rules to APP7.**

36. **APP8 needs updating to require consent express by a data recipient to send a customer's banking data overseas.**

37. **APP11 must be updated to ensure that consumers hold the right to delete data where:**

    a) **the data is no longer necessary in relation to the purposes for which it was collected;**

    b) **the individual withdraws consent or the relevant storage period has expired;**

    c) **the individual objects to the processing of data; or**

    d) **the data was unlawfully processed.**

38. **The charging of fees under APP12 should be removed for the purpose of the Open Banking Regime and for access to personal information more generally.**

39. **APP12 will need to be amended to include:**

    a) **permitting a request for access to information to come from a third party data recipient accredited under the Open Banking regime**

    b) **providing some reasonable limits to the right to refuse access to personal information for the purposes of the Open Banking regime;**

    c) **ensuring that the times involved in providing such access under the Open Banking regime are commensurate with the intent of the regime.**

40. **APP13 should be amended to ensure that data holders must take immediate steps to correct information once they become aware (by learning themselves or being told by the consumer) that personal information is inaccurate, out of date incomplete, irrelevant or misleading. Entities should be held liable for any reliance on this information that leads to a loss.**

Recommendation 4.3 – right to delete

41. **The right to deletion is integral for the Open Banking regime to work as currently recommended by the Report and must make up a part of the Consumer Data Right.**

Recommendation 4.6 – single screen notification

42. **Consents should be straightforward, meaningful, informative and unable to be relied upon by data recipients where the ultimate use in dispute is not expressly described in the consents but is merely implied or captured in a broad catch-all phrase.**

43. **Consents should be presented in plain language and data recipients should be prevented from using:**

    a) **pre-ticked boxes;**

    b) **negative sentences;**

    c) **silence or inaction;**

    d) **illegible terms and legalese**

    e) **or any other strategy meant to obscure the consent process.**

44. **Article 4(11), Article 7(3) and Recitals 32, 42 and 42 of the General Data Protection Regulation (GDPR) should act as the basis for consent regime under Open Banking.**

45. **The development of the consent protocols of the Open Banking regime should be consumer tested. The Behavioural Economics team of ASIC should be involved in the appropriate committees in the proposed Data Standards Body.**

46. **The regulator needs to undertake compulsory post-purchase/post-initiation audit surveys to find out what consumer believe that they have consented to and whether this aligns with the consents as formulated by the data recipient. A certain percentage of consumers should be required to have understood the consents.**

Recommendation 4.7 – joint accounts

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

Recommendation 4.9 – allocation of liability

48. The Report needs to consider the risk and liabilities that may arise from the on-sale or provision of a customer's data. We believe that third party data recipients must be held liable for any sale to fourth parties where it is reasonably foreseeable that a loss or breach of the Open Banking regime laws and regulations may occur. One solution that needs to be considered is requiring accredited entities from only selling or sharing data to fourth parties who adhere to the accreditation criteria themselves.

49. The liability principles put forward in the Report must be re-considered to ensure consumers are protected from the foreseeable negligence of data holders not keeping accurate, complete and up to date data records.

Chapter 5 – The data transfer mechanism

Recommendation 5.1 – application programming interfaces

50. The practice of screen scraping with respect to financial information should be outlawed.

Recommendation 5.2 starting point for the data transfer standards and Recommendation 5.3 - extensibility

51. The UK Open Banking technical specification should be used as the basis for standards for the data transfer mechanism, in line with the EU PSD2 regulatory technical standard for authentication and communications.

52. Extensibility should be built into the standards to ensure future functionality.

Recommendation 5.4 – customer-friendly authentication and authorization

53. A de-coupled approach as a starting point may be more prudent rather than the UK's redirect-based authorisation and authentication model but are not averse to further investigation and consideration of all models to ensure the highest level of security for consumers.

54. In developing the authentication and authorisation standards and process, the Data Standards Body should consumer test the API before settling on a final version. Involvement of the Behavioural Economics team of ASIC again is essential.

Recommendation 5.6 – persistent authorisation

55. Consumers should be able to:

    a) limit the authorisation period of their own choosing;

    b) be able to do so at any time, at their own discretion;

    c) revoke authorisation through the third party or via the bank data holder

    d) be notified periodically that they are still sharing information;

e) have the authorisation expire after a set period..

Recommendation 5.9 – access without online banking

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

Recommendation 5.10 – transparency

57. Consumer representatives support Recommendation 5.10

Chapter 6 – Implementation and beyond

Recommendation 6.4 – consumer education programme

58. Consumer representatives support Recommendation 6.4

Chapter 2: Open Banking Regulatory Framework

Recommendation 2.1 – a layered regulatory approach

Consumer Representatives support the recommended layered regulatory approach by implementing a broad Consumer Data Right under the *Competition and Consumer Act 2010*.

General Consumer Data Right

We note however that the Report does not detail the precise scope of the general Consumer Data Right. As we understand it the Government supports the implementation of a Consumer Data Right following a recommendation by the Productivity Commission's Data Availability and Use Inquiry. The right would enable consumers to control their data by allowing them to:

- share in perpetuity joint access to and use of their consumer data with the data holder
- receive a copy of their consumer data
- request edits or corrections to it for reasons of accuracy
- be informed of the trade or other disclosure of consumer data to third parties
- direct data holders to transfer data in machine-readable form, either to the individual or to a nominated third party.[2]

We support the creation of these general rights. However we disagree with the Productivity Commission's views with respect to the scope of this right by not including the right to erasure – a right that will be available to consumers in Europe under the General Data Protection Regulation (**GDPR**) from May 2018.

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

- the data is no longer necessary in relation to the purposes for which it was collected: Article 17(1)(a)
- the individual withdraws consent or the relevant storage period has expired and the data holder doesn't need to legally keep it (such as banking records for a seven time period): Article 17(1)(b)
- the individual objects to the processing of data – including direct marketing purposes and profiling: Article 17(1)(c) & Article 21
- the data was unlawfully processed: Article 17(1)(d)
- there is a legal requirement for the data to be erased: Article 17(1)(e)
- the consumer is a child at the time of collection: Article 17(1)(e) & Article 8

[2] p. 35 Productivity Commission, *Data availability and Use*, *Inquiry Report*, No. 82, 31 March 2017 https://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf

There are exceptions to this right, which include:

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

We note that the Productivity Commission's Data Availability and Use Report does not refer to this right when detailing its model for a comprehensive right, only mentioning it in a case study at the back of the report.[3] The Productivity Commission's discussion of this right is far from comprehensive, only detailing a little history, describing what it is, and then listing a few arguments against the need for such a right. There is no discussion on the clear and obvious policy and consumer protection reasons why the EU have decided to take this step. This is disappointing.

The arguments put forward against the right to erasure by the Productivity Commission are:

- the "right to be forgotten" is misleading as "information cannot be made deliberately forgotten – at best… information can be made less readily accessible."
- exercising the right to be forgotten may have the opposite effect by raising awareness of the information that the subject wishes to be forgotten;
- a takedown system may have an "undesirably chilling effect on online freedom of expression and any such power would need to balance the interests of the complainant against the interests of the party in publishing the material and broader public interests."
- a take down mechanism may be ineffective, particularly if located overseas.

We believe that these arguments do not stand under scrutiny, and apply to a limited understanding or conception of what the right to erasure applies to – that is the context of taking down defamatory material from search engines – and not personal information and data gathered by companies using digital applications.

With respect to the "at best - information can be made less readily accessible" argument, this may be the case with respect to defamatory material placed up on the web, it is not the case with respect to financial information provided to an accredited entity under an Open Banking regime. Accredited entities can retain full control, and if there are appropriate restrictions on selling or sharing this data to third or fourth parties (as the EU Right foresees: cf Article 21), then this control can be maintained.

[3] pp. 592-4, *Productivity Commission, Data Availability and Use Report*, https://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf

Similarly, in the context of defamatory material, exercising the right to be forgotten may indeed have the opposite effect by raising awareness of the information that the subject wishes to be forgotten. This however has not resulted in defamation laws being removed from the common law and statutes. This argument also does not apply to consumer data used in an Open Banking context or any number of contexts and uses in the current environment.

The chilling effect on broader public discussion also does not apply to data in the Open Banking context, nor does a take-down notice, which can be easily implemented in the Open Banking and Consumer Data Right environment.

There are many clear arguments for a right to erasure. These are mainly focussed on the privacy and security benefits it affords consumers increasingly concerned and impacted by data breaches and the increasingly unscrupulous and unbounded use of personal data. Objecting to your own personal data's use in direct marketing, being subject to the potential for identity theft or being subject to actual material theft through breaches of say financial details are all clear reasons for the right to erasure to be included under a Consumer Data Right.

More pertinent though is that the right to deletion is integral for the Open Banking regime to work as proposed. If consumers are to have confidence in the Open Banking regime, this distills down to the need to having control over their own data and to know that if they withdraw consent at any time that data will be deleted.

Consumers do not want the situation where their data has been used by a company – with or without consent – and that company holds on to that data to use for secondary purposes, either in aggregated or de-identified form where there is any possibility of re-identification. We discuss this issue further under *Recommendation 3.5 – aggregated data*. The recent news[4] that UK company Cambridge Analytica legitimately gathered some personal data from Facebook accounts and concurrently illegitimately gathered other people's data, and then, when found out and were requested to delete the data, did not, has raised public consciousness over the potential for data to be misused. Combined with the never ending list of significant and high profile data breaches at Equifax, Ashley Madison, Yahoo and more, the desire on the part of consumers to control their data via strengthened regulations is becoming stronger every day.

The Government will be opening consumers up to serious consequences if the right to erasure is not embedded within the regime from the very beginning. It risks undermining trust and confidence in a system it is promoting as the future. If a right to erasure is not included future headlines will include the names of accredited Open Banking entities rather than Facebook and Cambridge Analytica.

Furthermore, if the Consumer Data Right and the Open Banking regime does not include a right similar or the same to the EU GPDR, then Australian accredited entities with any interest in working internationally will need to create dual data handling protocols applying to

[4] '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

competing jurisdictions. This is a burden on innovation and will place Australian FinTechs at a distinct disadvantage to international competitors.

We note that with respect to the right to delete, the Report suggests that it is beyond the scope of Open Banking to mandate a special right to deletion of information.[5] We however strongly disagree and take the position that the right to deletion is integral for the Open Banking regime to work as currently recommended by the Report. It will also require the updating of the Australian Privacy Principles as discussed below under *Recommendation 4.2*.

Layered regulation

Consumer Representatives agree with the approach being put forward that establishes a Ministerial power to apply the CDR to designated sectors and datasets over time. From this, Rules will be set in subsidiary instruments by Government:

> *possibly through a regulator, or other arms length body – to balance competing interests and ensure that the views of all interested parties are heard. These parties would include participants, consumer groups, and technological and other relevant experts.*

It is critical that consumer groups be a part of this process and that a true balance of competing interests be encouraged. Consumer Representatives note that in the Open Banking space there are a significant number of parties seeking to protect or promote their financial interests. While competition is important to ensure better outcomes for consumers, the powerful interests of incumbent banks, and the potential start-up feeding frenzy of FinTechs promoted as "innovation" will be loud voices competing with consumers. It is therefore critical that consumer voices are sought out and supported to be involved in the rule making and standards setting processes as an important balance to essentially profit-driven perspectives. If Open Banking is to be truly customer focussed and be seen from the customer's perspective as put forward by this Report, the consumer voice must be embedded in every step of the Open Banking regime's development.

In order for this to occur we believe that under-resourced consumer organisations will need to be funded by the Government to provide the necessary input.

Recommendation

1. **Consumer Representatives support Recommendation 2.1's layered regulatory approach.**
2. **A right to erasure modelled on the EU GPDR should be included in the general Consumer Data Right empowering individuals to request the erasure of any links to, copy or replication of the data in question, where:**
   a) **the data is no longer necessary in relation to the purposes for which it was collected;**
   b) **the individual withdraws consent or the relevant storage period has expired;**

[5] Recommendation 4.3, p57, *Review into Open Banking: Giving customers choice, convenience and confidence*, December 2017, https://static.treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open-Banking-_For-web-1.pdf.

c) **the individual objects to the processing of data;**

d) **the data was unlawfully processed;**

e) **there is a legal requirement for the data to be erased**

f) **the consumer is a child at the time of the collection.**

3. **Consumer groups must be a part of the rule and standard setting process and should be appropriately resourced to do so.**

Recommendation 2.2 – the regulator model

Consumer Representatives support a government-led, multiple regulator model with the Australian Competition and Consumer Commission (**ACCC**) as the lead regulator to cover the expansive Consumer Data Right.

Consumer Representatives note that the report recommends that

> *"The OAIC should be responsible for ensuring that Open Banking is implemented in accordance with the Privacy Act and be the primary complaint handler (as customer complaints are likely to relate to privacy concerns.)"*

While in theory the Office of the Australian Information Commissioner (**OAIC**) should be the primary complaint handler for breaches of the *Privacy Act 1988* as they pertain to the overarching Consumer Data Right, we believe it is more appropriate that the newly created one stop shop for financial services complaints – the Australian Financial Complaints Authority (**AFCA**) – be the central point for receiving privacy breach complaints and all other complaints with respect to the Open Banking regime.

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

Lack of procedural clarity: We have not been given an overall explanation of how complaints would proceed from the outset, nor have we been told what the steps toward a determination would be, or the estimated timeframes for the various stages of a complaint.

Non-transparency: In one complaint, we were made aware of discussions that the Privacy Commissioner had with opposing parties regarding one of our complaints, including regulatory guidance that the Commissioner gave to representatives of the opposing party on issues of the complaint to which we were never made privy. We asked for transcripts of relevant meetings or at least a written summary of the issues discussed but we were never given anything.

Confidentiality: Consumer representatives have found that it has been unclear what parts of the complaints process were confidential and what parts were not confidential. A statement needs to be sent at the start of a complaint process by the OAIC to both parties to clarify this matter. The complaint process should be transparent.

Lack of timeliness: Consumer representatives have experienced significant delays between communications with the OAIC, had meetings cancelled with limited notice, and multiple deadlines given to opposing parties to respond to our complaints were ignored and unenforced. The opposing party in a series of complaints did not formally respond to any of them until eight months after consumer representatives lodged them with the OAIC. We have experienced delays of up to two years.

Unreasonable conciliation: We were also made to attend two separate conciliation meetings even though we made it clear in writing and verbally that we did not believe our complaints could be resolved in that manner, and we were unable to compromise on behalf of all the consumers that we represented in the proceedings.

Consumer Representatives acknowledge that, as noted in the Report:

> *The Information Commissioner can recognise external dispute resolution (EDR) schemes to handle particular privacy-related complaints. For the financial sector, the Credit and Investments Ombudsman (CIO) and the Financial Ombudsman Service (FOS) have been recognised as EDR schemes. Both the CIO and FOS are able to receive, investigate, facilitate the resolution of, make decisions and recommendations for, and report on, complaints about acts or practices of their members that may be an interference with the privacy of an individual. In the 2017-18 Budget the Government announced a new one-stop shop dispute resolution scheme, the Australian Financial Complaints Authority (AFCA), to replace the existing CIO, FOS and the Superannuation Complaints Tribunal. AFCA is expected to take steps to be recognised by the Information Commissioner as an EDR scheme.*

Given the deficiencies in the OAIC process described above, Consumer Representatives believe that if the OAIC is to be the "primary complaint handler" then an arrangement as currently exists with external dispute resolution (**EDR**) schemes needs to be implemented from initiation of the Open Banking Regime, in order that AFCA can handle all privacy-related complaints. It should be able to receive, investigate, facilitate the resolution of, make decisions and recommendations for, and report on, complaints about acts or practices of their members that may be an interference with the privacy of an individual.

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

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

Consumer representatives wish to also note that many FinTechs currently fall within the cracks of the current licensing schemes and requirements and therefore do not necessarily need to be members of an EDR scheme. Despite this we are aware of some that voluntarily choose to be. Consumer Representatives are also aware that the Parliament is currently

considering the amendments[6] which will be implementing FinTech Sandbox Regulatory Licensing Exemptions which will ensure that external dispute resolution will be available.

In order that there be clarity on this issue, it is critical that the accreditation criteria, described in the Report with respect to recommendation 2.8 include provisions that make membership of the AFCA compulsory. Consumer Representatives note that the Review recommends that

> *"the ACCC should consult with relevant sectors to determine criteria as part of the Rule setting process"*[7]

and that criteria *may* include the party being compliant with IDR and EDR processes. Consumer Representatives strongly believe that this must be implemented as a bare minimum.

Recommendation

4. **The ACCC should act as the lead regulator in a government led, multiple regulator model which include ASIC, AFCA and the OAIC to administer and enforce the expansive Consumer Data Right.**

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

6. **The accreditation criteria should include provisions to ensure membership of the AFCA be compulsory for all companies.**

Recommendation 2.3 – the banking Consumer Data Right

We support the sector by sector approach being proposed to implement the Consumer Data Right and support Open Banking being the first designated sector.

We would also note that one financial services sector that will require consideration for designation will be the insurance industry. Insurance is awash with data and is already fundamental to developing business models in the existing sector and the FinTech area. We believe that there may be great potential for a Consumer Data Right to improve consumer outcomes in insurance by:

- providing greater control over the use of personal data in the insurance space, where there is currently very few consumer protections;

[6] Treasury Laws Amendment (Measures for a later sitting) Bill 2017: FinTech Sandbox Regulatory Licensing Exemptions and the Treasury Laws Amendment (2018 Measures No. 2) Bill 2018

[7] p. 26, *Review into Open Banking: Giving customers choice, convenience and confidence*, December 2017, https://static.treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open-Banking-_For-web-1.pdf.

- improving the long battle of asymmetry of information in insurance;
- developing improved products and services;
- improving switching and competition issues; and
- preventing and negating the impact of price discrimination and risk discrimination that will develop as data and big data becomes more and more integral to the insurance sector's business model.

Recommendation

7. **The sector by sector approach to implement a Consumer Data Right is appropriate as is the choice to have Open Banking be the first designated sector.**

Recommendation 2.8 – the accreditation criteria

Consumer Representatives support the implementation of strong accreditation criteria to ensure consumer protections are built into the system from the start.

Consumer Representatives are not averse to a tiered model for accrediting entities on the basis of the potential harm that a relevant dataset and that party may pose to consumers and to the Open Banking system. However we do believe that – at least for the Open Banking system – there needs to be baseline criteria to which all tiers must adhere. These include:

- meeting privacy standards and security standards (as described below under *Recommendations 4.1-4.9*) including a description of the process in place to file, monitor, track and restrict access to consumer data;
- demonstrating that they have the technical capabilities to meet the standards,
- adhering to mandatory breach notifications;
- establishing risk management processes and measures including procedures to deal with security incidents;
- adhering to trust accounting rules and other measures taken for safeguarding payment service users funds;
- establishing Internal Dispute Resolution (**IDR**) process;
- membership of an EDR body ie. AFCA;
- processes that meet effective customer consent including testing procedures to demonstrate that customers understand what has been consented to;
- the collection of statistics/data on performance, transactions and fraud for the use of regulators;
- ensuring that all primary and secondary uses of any product or service meet a set of ethical standards or principles; and

- no history of data breach or misuse, or of disregard for the law.

We believe that the EU Payment Services Directive (**PSD2**) directive provides important guidance as to what should be included in accreditation criteria. Many of these should be able to be met by any potential FinTech wishing to engage in the Open Banking System. Many of them are included above but are simply basic business documentation including:

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

One key concern of consumer representatives is the business model of FinTechs particularly "Freemium" models that in part will make money from advertising or the sale of data and information to "fourth parties"[8] in Australia or overseas.

Any business model dependent upon the on-sale of personal data to fourth parties is one that has the potential to sell this data to any and all entities including unscrupulous or disreputable international or Australian parties who have a history of misuse of data through spamming, hacking or other activities that don't meet the law or community expectations. We believe that at minimum, the sale of this data to fourth parties needs to be regulated and overseen under the scheme. We would prefer the practice be banned outright.

This could be instituted in the accreditation criteria or made more explicit in the rules or standards. However this issue needs to be seriously considered by the Government, otherwise it is likely that this issue alone will undermine confidence in the entire Open Banking regime. We discuss this further under *Recommendation 4.9 - allocation of liability* below.

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

Consumer Representatives also note that defining high risk versus low risk for the purposes of a tiered accreditation system may be difficult. The Report refers to the concept of sensitive information in the *Privacy Act 1988* which we would argue this concept as currently conceived by the Act requires updating.

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

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

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

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

Sensitivity is, however, contextual. Certain information in the hands of one party may be mundane and uncontroversial but highly sensitive and consequential in others. The current definition of sensitive information in the Act does not include financial information, which is surprising and disappointing, notwithstanding the policy justification expressed above.

It is our view that their needs to be a full reconsideration of the concept of sensitivity under the *Privacy Act 1988* to ensure that financial data is also considered sensitive, less because of the chance of discrimination (although there is such a potential) but more because if it were to be breached, and not handled with appropriately high standards, it will lead to serious financial consequences.

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

Recommendation

8. Consumer representatives are not opposed to a tiered accreditation regime however there must be baseline accreditation criteria that all tiers must adhere including:

    a) meeting privacy standards and security standards (as described in Chapter 4 of the Report) including a description of the process in place to file, monitor, track and restrict access to consumer data;

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

    c) adhering to mandatory breach notifications;

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

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

    f) establishing Internal Dispute Resolution process;

    g) membership of an external dispute resolution body ie. AFCA;

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

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

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

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

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

9. The sale of this data to fourth parties needs to be regulated and overseen under the Open Banking regime. We would prefer the practice be banned

10. The concept of sensitive information, as defined under the *Privacy Act 1988* needs to be re-considered to ensure that financial information is appropriately protected.

Recommendation 2.9 Responsibility for the address book

Consumer Representatives support the creation of an address book (or whitelist) of accredited entitites. This should be maintained by the ACCC (or its authorised accreditors) and it should use block chain technology to ensure that it is not altered.

While an address book may be good for a consumer to go to to check, some form of reference to this address book should be made on the actual Open Banking service or product. While an accreditation logo or tick may or may not be the most appropriate way (but should be considered) at the very least, some reference and link to the address book should be included for consumers to check. Admittedly these links can also be spoofed, their presence may assist people to get used to the idea and recognise that there is an accreditation system ie a central, immutable, objective and independent site to go to confirm accreditation.

Recommendation

11. A public address book or white list should be made available and maintained by the ACCC. For the purposes of public education, an accreditation logo or tick should be considered for inclusion on all accredited products or services.

Recommendation 2.10 – Customer complaints and remedies

The successful implementation of a Consumer Data Right and an Open Banking system is dependent on the development of a strong consumer complaints approach that provides easy, straightforward access to justice.

It is important that there be a standardised IDR process for *all* accredited open banking parties, big or small. This should meet best practice as outlined in ASIC's *Regulatory Guide 165: Internal and External Dispute Resolution.*[9]

There must also be a clear EDR framework. In our view this is best done through an ombudsman service, rather than a regulator (like ASIC, or the OAIC) or a tribunal (such as the current Superannuation Claims Tribunal). This applies for both disputes that will arise for all Consumer Data Right issues across the economy and disputes arising from the Consumer Data Rights as it applies to Open Banking.

The key benefits of an ombudsman service are:

- greater accessibility and faster dispute resolution compared to legalistic tribunals;
- greater flexibility in resolving disputes, including resolving on the basis of what is fair and reasonable not just the law;

[9] http://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-165-licensing-internal-and-external-dispute-resolution/

- funding that comes from industry and responds to demand and does not depend on appropriation bills once this problem is no longer 'flavour of the month'; and
- an ability to respond to systemic issues, resolve the cause of consumer problems and facilitate consumer redress.

EDR in the financial system has provided access to justice for hundreds of thousands of consumers who would have been unable to resolve disputes if they had to rely on existing courts and tribunals, which are expensive, slow, and largely inaccessible without legal representation.

As we argued above, the complaints handling processes of the OAIC have left a lot to be desired and led to, in our view, a significant lack of access to justice for consumers.

Given this, Consumer Representatives believe that for the Open Banking system the AFCA should be the single contact point. Given the Government has just developed the AFCA in order to create a one-stop shop for complaints, it seems counter to this policy to now introduce another venue to deal with the privacy-related complaints arising from Open Banking. The services provided by Open Banking participants will be considered, rightly in our view, financial services and consumers will have an expectation that their complaints will be handled by the financial services sector independent referee, ie AFCA. Given the overlapping issues of privacy, and confidentiality with financial services, capability and competition, it seems to us that AFCA must be the external dispute resolution body to handle these issues.

If, as also argued above, the OAIC is to be the "single consumer data contact point," then AFCA should be recognised by the OAIC at the EDR scheme to handle privacy and consumer data right related complaints arising in the Open Banking system. AFCA should be able to receive, investigate, facilitate the resolution of, make decisions and recommendations for, and report on, complaints about acts or practices of their members that may be an interference with the privacy of an individual.

We agree with both the Report that there should be "no wrong door" for consumers. If they approach the OAIC they will be sent to AFCA, if they approach AFCA they will have their complaint handled.

We believe that the Australian Privacy Principles and the *Privacy Act 1988* must be updated and strengthened alongside the development of the Open Banking system. See further information on this below under *Recommendation 4.2*.

Recommendation

12. A standardised, IDR process for *all* accredited open banking parties, big or small must be mandated and should meet best practice as outlined in *ASIC's Regulatory Guide 165: Internal and External Dispute Resolution*.

13. A one stop EDR framework based on the ombudsman model is essential for consumers to have access to justice. This should be AFCA. We agree with the Report that there should be "no wrong door" for consumers..

Enforcement

Consumer Representatives note the recommendation that the ACCC should have broad research and investigative powers, and that they should be provided with a range of remedies to enforce the Consumer Data Right. These would include directions powers for the deletion of data, audits, reviews and compensation orders, criminal penalties, amongst many listed at page 31 of the Report. We support the implementation of this enforcement power.

We believe that for regulation and enforcement to be effective there should be significant penalties for breaches to accreditation criteria, the APPs and the Consumer Data Rights to redress, including disgorgement remedies. If the Consumer Data Right will be applied under the *Competition and Consumer Act 2010*, then we presume all penalties and remedies regime should apply to breaches of the law.

Recommendation

14. **A strong and wide-ranging research, investigation and enforcement regime should be included in the Open Banking regime, with ACCC empowered with an expansive regulatory tool-kit.**

15. **There should be significant penalties and remedies for breaches to the Consumer Data Right and the Open Banking regime, as per the *Competition and Consumer Act 2010*.**

Chapter 3 – The scope of Open Banking

Recommendation 3.1 – customer-provided data

Consumer representatives support data holders being obliged to share all information that has been provided to them by the customer (or a former customer) except for information supporting an identity verification assessment. We agree that data holders should only be obliged to share identity verification information with the customer directly, not a data recipient. We support examining the Anti-Money Laundering Laws to consider whether a data recipient can rely on the identification procedures of a third party.

Recommendation

16. Consumer representatives support recommendation 3.1.

Recommendation 3.2 – transaction data

Consumer representatives support data holders sharing transactions relating to banking deposit and lending products listed in the Report. We would note that Treasury may wish to consider new forms of credit and debit-like accounts that are developing such as By Now Pay Later platforms such as Afterpay and Certegy.

Recommendation

17. Consumer representatives support recommendation 3.2 but may wish to consider new forms of credit and debit-like accounts that are developing such as By Now Pay Later platforms.

Recommendation 3.3 – Value-added customer data

The Report states that value added customer data refers to data that has been created by the data holder:

> *through the application of insight, analysis or transformation of a customer's transaction data to enhance its usability and value"*[10]

[10] p. 37, Review into Open Banking: Giving customers choice, convenience and confidence, December 2017, https://static.treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open-Banking-_For-web-1.pdf

The Report goes onto say that:

> *While this derived data would not have been able to be created without the customer, its value has largely been generated by the actions of the data holder, or has been externally augmented by authorised data recipients (such as credit bureaux). As such imposing an obligation to share that data may amount to a breach of intellectual property rights.*[11]

It's important to be clear about the type of data we are talking about here: data holder banks can and are creating profiles of individual users based on an analysis of the data they hold and potentially matching it with other data sources they have created or have purchased (such as social media data).

From this, data holder banks can gain a multitude of insights into an individual's behaviour: who buys what, when, at what price, their credit-worthiness, their loyalty to businesses and 'stickiness,' their relationships, their attitudes, even political opinions (arising out of say an ongoing debit to the Liberal Party of Australia or the Greens). All of these data points paint a significantly unique and valuable picture of every one of their customers. Subsequently, banks can link these to internal or third party marketing initiatives, product development, and sales or suggestions for new products or needs.

Many of these uses of value added data may in fact be good. Gaining an insight into a bank customer experiencing, say, financial hardship, could allow banks to take proactive steps to assist the customer by suggesting a financial hardship variation on a mortgage or to offer to shift the customer into a low fee account. At the same time though, banks could potentially use this data to push products that may not in fact be appropriate, such as pushing low value add-on insurance products including CCI, or selling the data to a third party debt management firm or pay day lender to subsequently market to them.

This ability to target will also potentially lead to price discrimination on a broad scale.

Consumer representatives do not support value-added data being included in the scope of the Open Banking regime. However we do wish to strongly put the position that value added data should be shared with the consumer for the sake of transparency. Consumers should have access to the types of insights that a data holder is creating and for what purposes they are using this data.

We note for example that Facebook has a feature called "Your ad preferences"[12]- where they tell you what types of insights they have gained on the user for the purpose of advertising. It lists, "Your interests," "Advertisers you've interacted with" and "Your information" which includes the particularly interesting "Your categories" featuring all the categories that Facebook have algorithmically placed you into to:

> *help advertisers reach people who are most likely to be interested in their products, services and causes. We've added you to these categories based on information you've provided on Facebook and other activity.*

---

[11] p. 37, *Review into Open Banking: Giving customers choice, convenience and confidence*, December 2017, https://static.treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open-Banking-_For-web-1.pdf.

[12] https://www.facebook.com/ads/preferences

They can include, for example:

- Birthday in March
- Early technology adopters
- Gmail user
- Safari Browser user
- Likely to engage in Politics (conservative)
- Frequent traveler
- Away from home town
- Close friends of women with a birthday in 7-30 days.

As an example of corporate transparency, this provides a model for what will become expected for all data holders. We believe that as a part of the Open Banking regime and the Consumer Data Right, consumers should be, at the very least, able to see what types of insights the Bank has created in developing value added data and what uses these insights are being put.

Why is this important? Other than the basic right of consumers to know what is being done with the data held on them, it is also important for competition purposes. Lauren Solomon of the Consumer Policy Research Centre writes:

> *One fundamental criterion of perfect competition is perfect information: that both buyer and seller have perfect or complete information about the transaction…. When sellers have more information than buyers about the transaction, …this can lead to "adverse selection", with buyers often ending up with a lemon of a used car.*
>
> *Consumer data, when amalgamated, can absolutely increase the knowledge of the seller, which would suggest an increased likelihood of adverse selection due to the knowledge and power imbalances inherent in the trade.*[13]

If as the Report states as one of the four key principles of the Open Banking regime is to encourage competition – ie "it should be done to increase competition for the banking products and services available to customers so that customers can make better choices" – then it is critical that both the data holder and the consumer have the same information, otherwise the Open Banking regime will embed and heighten information asymmetry rather than improving it, which neither serves competition nor improves consumer outcomes.

Recommendation

18. Consumer representatives do not support value-added data being included in the scope of the Open Banking regime.

[13] Lauren Solomon, It's time for Australia to think magna data, *The Mandarin*, 20 February 2018 https://www.themandarin.com.au/88674-time-australia-think-bigger-big-data/

19. **Value-added data should be shared with the consumer for the sake of transparency. Consumers should have access to the types of insights that a data holder is creating and for what purposes they are using this data.**

Recommendation 3.5 – aggregated data

According to the Report, aggregated data is data that is:

> *created when banks use multiple customer's data to produce de-identified, aggregated or averaged data across customer groups or subsets.*[14]

We are concerned that the definition of aggregated data sets used in the Report is not precise enough. There are (1) aggregated data sets (2) de-identified aggregated data sets, and (3) the summary data that they can produce – seemingly referred to as "aggregated data" in the report. We presume the Report is defining "aggregated data" as a combination of the latter two.

It is important to be clear on what is meant by aggregated data sets because of their fundamental privacy and security implications. To provide further context we refer to Boris Lubarsky's[15] five levels of data identifiability. These are:

1. Direct identifiers: Name Address, Medicare number, Bank account number
2. Indirect identifiers: Date of birth, postcode, licence plate, IP address
3. Data that can be linked to multiple individuals: shopping preferences, physical measurements
4. Data that can't be linked to any individual: aggregated census data or survey results
5. Data not related to individuals: weather and geographic data

Lubarsky then proceeds to delineate four types of data scrubbing:

1. Removing data (eg remove or redacting names)
2. Replacing data with pseudonyms
3. Adding statistical noise
4. Aggregation with summary data produced eg releasing the total number of people who have a particular bank account.

If a dataset is de-identified it fits into categories 1 to 3 as forms of de-identification. If it is aggregated, averaged or summarised it falls into category 4.

---

[14] p. 39, *Review into Open Banking: Giving customers choice, convenience and confidence*, December 2017, https://static.treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open-Banking-_For-web-1.pdf

[15] Boris Lubarsky, Re-identification of "Anonymized Data, *Georgetown Law Technology Review*, 1 GEO. L. TECH. REV. 202 (2017) https://www.georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017/

This is important because there is a potential for de-identified datasets to be re-identified. According to Lubarsky:

> *Data re-identification occurs when personally identifying information is discoverable in scrubbed or so-called "anonymized" data. When a scrubbed data set is re-identified, either direct or indirect identifiers become known and the individual can be identified.*

Lubarsky raises three ways to re-identify:

1. insufficient de-identification: when a direct or indirect identifier inadvertently remains in a data set that is made available to the public
2. pseudonym reversal: when a key" is kept to reverse the process, or the method used to assign pseudonyms is discovered or becomes know the data can be re-identified
3. combing datasets: where two datasets that contain the same individual(s) in both sets are combed to re-identify.

Aggregated data sets (de-identified, anonymised, pseudonymised, summarised or otherwise) are regularly sold and transmitted to third parties, such as analytics companies, marketing companies, or commercial data brokers. However given the power of big data analytics and the availability of publicly available information and other similar data sets, it is now possible to re-identify individuals when combined. This has significant privacy implications, particularly with respect to sensitive information and financial information.

The EU GPDR law has simplified the issue by focussing on the concepts of "anonymous data" and "pseudonymous data". The EU concept of "anonymous data" is only considered as such if re-identification is *impossible* , that is, re-identifying an individual is impossible by any party and by all means likely reasonably to be used in an attempt to re-identify.[16] Further, "pseudonymous data" is defined as

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

The GPDR will permit data holders to process anonymous data *and* pseudonymised data for uses beyond the purpose for which the data was originally collected.[17] Recital 78 and Article 25 in fact foresee pseudonymisation as a method to demonstrate compliance with Privacy by Design requirements, a concept we have recommended in previous submissions and continue to do so. However Recital 26 limits the ability of data holders benefiting from pseudonymised data if re-identification techniques are "*reasonably likely* to be used, such as singling out, either by the controller or by the person to identify the natural person directly or indirectly." In other words, if de-identified aggregate data is reasonably likely to be re-identified, it cannot be used by the data holder. The EU Article 29 Working Party has yet to release guidance on pseudonymisation and what techniques may be appropriate to use. The GPDR has yet to

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

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

become effective – which it will on 25 May 2018, so there is no evidence yet to see how this will work practically.

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

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

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

Recommendation

20. **Aggregated data sets should not be included in the scope of Open Banking.**
21. **Consumers should be able to withdraw consent for the use of aggregated data sets by a data-holder (or recipient) and that this data be destroyed.**
22. **The concepts of anonymised data (where re-identification is impossible by any party by any means) and pseudonymous data (except re-identification techniques are reasonably likely to be used) as per the GPDR should be embedded in the Consumer Data Right and the Open Banking regime.**
23. **Consumers should be fully informed and provide express consent to all uses of aggregated datasets (de-identified or otherwise), including who has access to them.**

Recommendation 3.7 – application to accounts

Consumer representatives note that the intent of the Open Banking regime is to ensure that all customers – individuals, small business and large businesses have access to the regime. While we generally support this we wish to raise one issue that needs to be considered and that relates to age.

Are children able to provide the required informed and express consent to the use of Open Banking products? Consumer representatives have not considered the issue much ourselves but we raise it in the light of a recent case involving a new By Now Pay Later service.

Case Study – Jane's story - C159145

Jane applied for a By Now Pay Later Service in about Jan 2017 to purchase some goods at Retailer 1. At the time she was only 17, a student and was working one, sometimes two days per week After having partially paid that off this first purchase in May 2017 Jane used the By Now Pay Later Service again at Retailer 2's website in order to buy a watch and some other goods which totalled about $400. She contacted Financial Rights in she was no longer working because she had been involved in a car accident.

Jane's mother helped to pay some of her debt but Jane's mother is also unemployed and can no longer afford to help. The balance owing on Jane's Afterpay account is approx $280 and she thinks she is attracting $10 late fees every time she fails to pay. Jane is struggling with several other debts including damages from a car accident and has no capacity to pay off her Afterpay debt.

Jane says the application form only asked her for personal details such as name, address and phone number. There is an 18 years old age limit on the Buy Now Pay Later Service. There were no questions about her employment or income. At the time of applying for the Buy Now Pay Later she was working one to two shifts at Coles as a casual earning $100/week.

Source: Financial Rights Legal Centre

We believe serious consideration needs to be given to the impact of Open Banking on young people – be it aged 18, 16 or younger and investigate the issues that need to be addressed. Young children may be particularly vulnerable to new apps and may not fully understand the consequences of consents required.

FinTechs may need to demonstrate that they have verified someone's age and identity before acquiring consent to share Open Banking data. We recommend the reviewers reach out to Youth Action NSW who has done advocacy on young person consent issues.

We note too that the EU's GDPR will restrict the ability to consent to those 16 years or potentially 13 years and above depending on the State:

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

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

We believe as a starting point similar restriction should apply both to the Open Banking regime and the Consumer Data Right.

Recommendation

24. **Consumer representatives support recommendation 3.7 but recommend a consideration of the impact of Open Banking services on young people, including restrictions similar to Article 8 of the GPDR.**

Recommendation 3.11 – no charge for customer data transfers

Consumer Representatives support there being no charge for customer data transfers.

Recommendation

25. **Consumer representatives support recommendation 3.11 that there be no charge for customer data transfers.**

Chapter 4 – Safeguards to inspire confidence

Recommendation 4.1 – application of the Privacy Act

Consumer Representatives support ensuring that all data recipients be subject to the *Privacy Act 1988*.

26. Consumer representatives support recommendation 4.1 that all data recipients be subject to the *Privacy Act 1988*.

Recommendation 4.2 – modifications to privacy protections

Consumer Representatives strongly support modifying and modernising the *Privacy Act 1988* including the Australian Privacy Principles. The last time privacy laws in Australia were comprehensively reviewed was ten years ago when the Australian Law Reform Commission wrote its report on Australian Privacy Law and Practice.[18] The way Australians use and supply data has changed dramatically in the last decade.

We provide the following comments and recommendations.

APP 3 – Collection of solicited personal information

We support the APP3 being amended to ensure that an entity must not collect personal information unless the entity can demonstrate that express consent has been received from the customer. We would recommend that APP3 make it clear that express consent must be:

- explicit;
- discrete for every use, purpose or function – that is, not bundled in any form
- fully informed;
- able to be permitted or constrained according to the customer's instructions including easily withdrawn with immediate effect and deletion of data.
- time limited.

The bundling of consents has been the bane of consumers for many years.[19] The *Privacy Act 1988* was drafted during a period where the use of digital terms and conditions that are bundled and lengthy were relatively new. Their use has led to a significant asymmetry of

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

[19] See CHOICE, Nine hours of 'conditions apply' 2017, https://www.choice.com.au/about-us/media-releases/2017/march/nine-hours-of-conditions-apply

information and power, working against the interests of consumers. They are unfair and have led to lower levels of product, service and data literacy.

The APP3 must be modernised and future-proofed with clear requirements on all companies (not just those involved in the Open Banking regime) to gain express, fully informed consent from consumer. The consents must be appropriately broken down for different types of data (bank account, transactional, credit card, repayment history, social, imputed and other general data), and uses (credit checks, marketing etc). This separating out of specific consents should not be solely limited to marketing. It should be applied to all types and uses of data including the on-sale of data.

The APP3 must also ensure that data recipients explain in simple, clear, terms why information is being collected and for what it is being used. Data recipients must be obliged to only collect the minimum amount of personal information that the business actually needs. This means not collecting extra information simply for marketing purposes at some later date, for example.

It is also important that the lack of consent should not limit the ability to receive the service unless the data is fundamentally necessary to the working of the product or service.

APP 4 – Dealing with unsolicited personal information

Consumer representatives support amending APP3 to ensure that a data recipient who has received unsolicited banking data will need to either gain express consent or be required to destroy or de-identify the unsolicited personal information.

APP 5 – Notification of the collection of personal information

We agree that the reasonable steps standard under APP5 is in no way appropriate for the Open Banking regime or for the future of the Consumer Data Right moving into the future. This too must be modernized and *require* notifications be made, with these notifications acknowledged and recorded. If there is to be any building of trust and confidence in the Open Banking system and the use of consents for the collection of personal information, it is critical that genuine actual notification and disclosure be embedded into the regime.

APP 6 – Use or disclosure of personal information

We strongly support ensuring that a data recipient demonstrates that any secondary use is directly related to the primary purpose. This link between the primary and secondary must not be spurious or trivial. There must be a clear, demonstrable link between the secondary purpose and the primary purpose.

APP 7 – Direct Marketing

We believe that significant restraints must be placed upon on the disclosure or use of personal data for direct marketing purposes. The current APP7 is manifestly inadequate.

At a minimum we support the recommendation in the Report that customers must provide their express consent before a data recipient can directly market to the customer. This should

not be bundled with other consents, consistent with our position above that all consents for distinct uses not be bundled.

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

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

We also believe that this section needs to be either extended or a new section created, regulating the on-sale of personal data provided to the data recipient and created by the data recipient through the customer's use of the product or service.

It is important that the choice to consent to these uses be a genuine choice and not one where consumers must choose between their privacy or potential exploitation. As Nic Dillon recently wrote:

> *In practice the Consumer Data Right will penalise people who want to protect their privacy. If other people choose to share their data – and you choose not to share yours – you can end up paying more for the same service. This means you pay for privacy. And if you can't pay with dollars, you'll pay with data.*[20]

APP 8 – Cross-border disclosure

As noted above, we strongly believe that consent must be sought and received by a data recipient before sending a customer's banking data overseas. We believe that the obligation on a data recipient to take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the data should be maintained and bolstered to make it so that the data recipient must ensure that this is the case.

Sending data overseas is and will be the biggest and most obvious chink in the safety and security regime in handling personal data collection. Firstly the data can become subject to the laws of the overseas jurisdiction, such as the United States, and be accessed under their laws. Secondly, if any breaches were to occur in an overseas jurisdiction it may be more difficult to access justice for somebody in Australia, particularly if that data is being on-sold to a fourth party based solely in another jurisdiction.

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

[20] Nic Dillon, "The Consumer Data Right: putting a price on privacy" *The Mandarin* https://www.themandarin.com.au/89051-consumer-data-right-putting-price-privacy/ b

APP 11 – security of personal information

While not listed in the table on pages 55-56 of the Report, Consumer Representatives believe that APP11 must be updated to ensure that consumers hold the right to delete data where:

- the data is no longer necessary in relation to the purposes for which it was collected;
- the individual withdraws consent or the relevant storage period has expired;
- the individual objects to the processing of data; or
- the data was unlawfully processed.

We have provided further details on this issue above at *Recommendation 2.1 – a layered regulatory approach* and under *Recommendation 4.3 – right to delete.*

APP 12 – access to personal information

Customer representatives note that the Report raises significant issues with the current APP 12 with respect to the charging of fees to access personal information. Currently APP 12 states that an organisation may charge an individual but that it must not be excessive and must not apply to the making of the request.

We strongly believe that this needs to be removed moving forward as a cost of business – both for the purpose of the Open Banking Regime and for access to personal information more generally.

Charging a fee to access your own personal information is already and will increasingly become a significant barrier to access. Whether a fee is excessive or otherwise is in the eye of the beholder and for particularly vulnerable consumers experiencing significant financial hardship, any fee, no matter how small it seems to others, will be too much and act as a barrier to such access. This principle is therefore embedding a class system for accessing private information. Even if a waiver were to be made available, this would be an additional hurdle to a cohort of consumers who, going on past experience, will simply not take the steps required.

We believe that the APP 12 must be amended to ensure that the process for gaining access to your own personal information should be easy and straightforward. It is a difficult task for an individual to request access to personal information as it is varied, generally hidden in terms and conditions or buried in the fine print somewhere on a website. Minimum standards need to be set.

We agree that in order for the Open Banking regime to work the APP12 will need to be amended to include:

- permitting a request for access to information to come from a third party data recipient accredited under the Open Banking regime
- providing some reasonable limits to the right to refuse access to personal information for the purposes of the Open Banking regime;
- ensuring that the times involved in providing such access under the Open Banking regime are commensurate with the intent of the regime.

APP 13 – correction of personal information

Consumer representatives can attest to a general ongoing failure to amend or correct personal information in a speedy or good faith manner. Seeking amendments to credit reports, as an example, is frustrating and difficult. And seeking corrections is important as inaccurate information can lead to say, losses under the Open Banking regime, notices being sent to incorrect addresses and the consequent losses that arise from that.

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

It is critical that APP 13 be amended to ensure that a data holder must take immediate steps to correct information once it becomes aware (by learning itself or being told by the consumer) that personal information they hold is inaccurate, out of date incomplete, irrelevant or misleading. If they do not they should be held liable for any reliance on this information that leads to a loss.

Recommendation

27. **APP3 must be updated and amended to ensure that an entity must not collect personal information unless the entity can demonstrate that express consent has been received from the customer which is:**

    a) **explicit;**

    b) **discrete for every use, purpose or function – that is, not bundled in any form**

    c) **fully informed;**

    d) **able to be permitted or constrained according to the customer's instructions including easily withdrawn with immediate effect.**

    e) **time limited.**

28. **APP3 must also ensure that data recipients explain in simple, clear, terms why information is being collected and for what it is being used. Data recipients must also be obliged to only collect the minimum of personal information that the business actually needs.**

29. **APP3 must also make clear that the lack of consent should not limit the ability to receive the service unless the data is necessary to the working of the product or service.**

30. **APP4 must be amended to ensure that a data recipient who has received unsolicited banking data will need to either gain express consent or be required to destroy or de-identify the unsolicited personal information.**

31. **APP5 must be modernized to require notifications to be made, acknowledged and recorded.**

32. **APP6 must be updated to ensure that a data recipient should demonstrate that any secondary use is directly related to the primary purpose.**

33. **APP7 should be updated to require customers provide their express consent before a data recipient can directly market to the customer. This should not be bundled with other consents.**

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

35. **The on-sale of personal data provided to the data recipient and created by the data recipient through the customer's use of the product or service should be covered by similar rules to APP7.**

36. **APP8 needs updating to require consent express by a data recipient to send a customer's banking data overseas.**

37. **APP11 must be updated to ensure that consumers hold the right to delete data where:**

    a) **the data is no longer necessary in relation to the purposes for which it was collected;**

    b) **the individual withdraws consent or the relevant storage period has expired;**

    c) **the individual objects to the processing of data; or**

    d) **the data was unlawfully processed.**

38. **The charging of fees under APP12 should be removed for the purpose of the Open Banking Regime and for access to personal information more generally.**

39. **APP12 will need to be amended to include:**

    a) **permitting a request for access to information to come from a third party data recipient accredited under the Open Banking regime**

    b) **providing some reasonable limits to the right to refuse access to personal information for the purposes of the Open Banking regime;**

    c) **ensuring that the times involved in providing such access under the Open Banking regime are commensurate with the intent of the regime.**

40. **APP13 should be amended to ensure that data holders must take immediate steps to correct information once they become aware (by learning themselves or being told by the consumer) that personal information is inaccurate, out of date incomplete, irrelevant**

or misleading. Entities should be held liable for any reliance on this information that leads to a loss.

Recommendation 4.3 – right to delete

Consumer representatives strongly support the right to erasure under the Consumer Data Right and believe it must be applied to the Open Banking regime, as argued above under *Recommendation 2.1 – a layered regulatory approach*.

As the Report notes, Open Banking will give a customer the right to be able to:

> *readily withdraw their consent or limit the time in which a data recipient can receive their data. Once the customer consent is withdrawn or expires, a customer would reasonably expect that their banking data would be deleted or destroyed in order to protect their privacy.*[21]

It is only practical therefore that the right to delete (or right to erasure) be embedded in the Consumer Data Right and Open Banking regime from the start, or else the above cannot be actioned. As the Report also points out this right currently does not exist under the APPs. APP 11.2 states that

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

There is no right to instruct deletion under this principle. It therefore is not capable of supporting a consent regime, as proposed in this report where they can readily withdraw their consent with immediate effect. Holding on to this data would negate this principle.

While the Report states that it is beyond the scope of Open Banking to mandate a special right to deletion of information, we believe it must make a statement in support of this principle in order for proper functioning of the Open Banking regime. The right to deletion is integral for the Open Banking regime to work as proposed.

As detailed above, if consumers are to have confidence in the Open Banking regime, this distills down to the need to have control over their own data and to know that if they withdraw consent at any time that data will be deleted.

[21] p. 57.

Recommendation

41. The right to deletion is integral for the Open Banking regime to work as currently recommended by the Report and must make up a part of the Consumer Data Right.

Recommendation 4.5 – customer control

We refer to the above discussion under *Recommendation 4.2* and *4.3* but reiterate we believe that the APP 3 must be amended to ensure that both the Open Banking Regime and consent more generally is updated to ensure that an entity must not collect personal information unless the entity can demonstrate that express consent has been received from the customer which is:

a) explicit;

b) discrete for every use, purpose or function – that is, not bundled in any form

c) fully informed;

d) able to be permitted or constrained according to the customer's instructions including withdrawn with immediate effect ie. the deletion of data; and

e) time limited.

The consent regime must also ensure that data recipients explain in simple, clear, terms why information is being collected and for what it is being used. Data recipients must also be obliged to only collect the minimum of personal information that the business actually needs.

Consent must be explicitly and discretely sought for every separate primary and secondary purpose including but not limited to marketing and the on-selling or sharing of a consumer's data and the sending of a consumer's data overseas.

The consent regime must also make clear that the lack of consent should not limit the ability to receive the service unless the data is necessary to the working of the product or service.

We also refer you to the discussion under the following section with respect to our views on some of the specifics of consent.

Recommendation 4.6 – single screen notification

Consumer Representatives agree that a data holder should assist in educating the consumer and notify that a request to share data with a data recipient has been received.

We do have one issue with the notification stating that "they cannot hold the data holder responsible once their direction has been made and complied with." While we generally support this basic notion of liability, as will be discussed further below, consumer representatives have serious concerns with some aspects of the liability schema being

proposed. Specifically, we have issues with mistakes or negligence a data holder may have made upon which data recipients and customers rely upon.

While we agree that this notification should not "add undue friction or impede a customer's willingness" we do not believe that friction is in itself necessarily a bad thing.

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

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

This is all the more important when it comes to the other end of the transaction where data recipients will gain consent from the consumer.

We agree that data recipients will need to facilitate a customer's ability to self select from a list of possible uses of their data.

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

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

Furthermore the consents should be presented in plain language and data recipients should be prevented from using some of the tricks of the trade that we have seen in other areas. These include the use of:

- pre-ticked boxes;
- negative sentences;
- silence or inaction;
- illegible terms and legalese

Article 4(11) of the GDPR establishes an opt-in consent that avoids many of these issues. Specifically, it states:

> *'consent' of the data subject means any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;*

It then goes on to clarify the meaning of clear, affirmative action, in Recital 32:

> *Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.*

It is also critical that that the consents are intelligible, easily accessible, use clear and plain language and it should not contain unfair terms. In line with Recital 42 and 43 consent should be freely given:

> *42. Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC[1] a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.*
>
> *43. In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.*

We strongly believe that these should be the standards for customer control in Australia.

We also agree that technology should allow a customer to terminate a data sharing arrangement at any time though both the data holder and data recipient's platform. This conforms to Article 7(3) of the GPDR:

> *The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.*

In order for the consent regime to work, the regulator needs to undertake post-purchase/post-initiation audit surveys to find out what consumer believe that they have consented to and whether this aligns with the consents as formulated by the data recipient. We believe that this post-initiation audit would be compulsory, conducted independently and require a certain percentage of consumers to have understood the consents, otherwise, data recipients will need to improve their consent and have increased monitoring to ensure their consent process meets best practice.

Furthermore it is prudent for the Data Standards Body in developing the consent regime and applications are consumer tested before settling on a final version. This should not be used to delay the process and can be done relatively easily and quickly, especially if the Behavioural Economics team of ASIC, established in 2014, is involved from the very beginning.

Recommendation

42. Consents should be straightforward, meaningful, informative and unable to be relied upon by data recipients where the ultimate use in dispute is not expressly described in the consents but is merely implied or captured in a broad catch-all phrase.

43. Consents should be presented in plain language and data recipients should be prevented from using:

- **a) pre-ticked boxes;**
- **b) negative sentences;**
- **c) silence or inaction;**
- **d) illegible terms and legalese**
- **e) or any other strategy meant to obscure the consent process.**

44. Article 4(11), Article 7(3) and Recitals 32, 42 and 42 of the General Data Protection Regulation (GDPR) should act as the basis for consent regime under Open Banking.

45. The development of the consent protocols of the Open Banking regime should be consumer tested. The Behavioural Economics team of ASIC should be involved in the appropriate committees in the proposed Data Standards Body.

46. **The regulator needs to undertake compulsory post-purchase/post-initiation audit surveys to find out what consumer believe that they have consented to and whether this aligns with the consents as formulated by the data recipient. A certain percentage of consumers should be required to have understood the consents.**

Recommendation 4.7 – joint accounts

While Consumer Representatives generally support the recommendation to ensure that each joint account holder should be notified of any data transfer arrangement initiated on their accounts and given the ability to readily terminate any data sharing arrangements initiated by any other joint account holders, we have concerns that this may be problematic in a domestic or family violence context.

We believe that any regulations, rules or standards developed with respect to joint accounts should be designed with family violence issues in mind.

Why is this important? As the Economic Abuse Reference Group (EARG) states:

> *Family violence can have a significant detrimental impact on a woman's financial wellbeing, both during the violent relationship, and if (and when) a woman leaves the perpetrator. Financial insecurity is one reason a woman may stay in a violent relationship. Leaving a violent relationship must sometimes be done quickly and suddenly. A woman may not be able to take much with her, or may have to move far away from her home due to safety concerns. This can leave a family violence survivor (and often her children) with few financial resources and make it difficult to find secure housing and establish a new life.*[22]

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

- incur debt for which she does not receive a benefit, or take on the whole debt of a relationship;
- relinquish control of her assets or income, or reduce or stop paid employment;
- claim social security payments;
- sign a contract, loan application or guarantee;
- sign documents to establish or operate a business;
- preventing access to joint financial assets, such as a joint bank account, for the purposes of meeting normal household expenses;
- demanding disclosure of a person's credit card details and/or passwords;
- demanding cash;

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

- preventing access to online banking or purchasing;
- preventing someone from seeking or keeping employment.

There may very well be potential problems arise out of Open Banking. These could include:

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

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

Recommendation

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

Recommendation 4.9 – allocation of liability

On-sale or provision of data to a "fourth party"

We note that the Report details a list of risks and liabilities issues that may arise. We recommend the Report consider another risk and liability that may arise under the Open Banking regime. That is, the situation where a customer's data is on-sold or provided to a fourth party, that may lead to problems ranging from identify theft and material theft to direct marketing and spamming.

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

We believe that one way to prevent issues arising is potentially requiring accredited entities from only selling or sharing data to fourth parties who adhere to the accreditation criteria themselves.

The Open Banking liability principle

We are concerned with the principle drawn from the scenarios listed in the report, that is, "participants in the Open Banking system should be liable for their own conduct but not the conduct of other participants in the system."

While this seems straightforward on the surface, it unfortunately leads to an absurd outcome with respect to at least one of the scenarios outlined in the Report. The scenario reads:

> *A customer directs their bank to share their data with an accredited data recipient. The data is inaccurate, incomplete or misleading and the data recipient relies on it for the purpose of offering a product to the customer. The product is offered on the basis of misleading information and the customer suffers a loss.*[23]

Under the current application of the banking law framework,

> *The bank could be responsible to the customer for inaccuracy of the records it keeps for its customer.*

However under the proposal the Report suggests that:

> *The bank should not be liable for the loss suffered on the product offered by the data recipient. The bank should be responsible to its customer for the correction of its records.*

This, in our view, is unjust.

While it is not made explicit in the Report, it is implied that the data recipient is deemed not liable for the loss in this situation. This is fair given they have relied on data that has been provided to them by a bank with consent from the customer.

We believe if the principle that "participants in the Open Banking system should be liable for their own conduct" holds then if the data holder has not acted to correct inaccurate, incomplete or misleading data as required under APP 13, then the data holder must be liable for the subsequent loss in this scenario.

The suggested result in the Report is one where the bank is merely responsible to correct records but not for the consequences of the breach of duty to take reasonable steps to ensure the data is accurate, up to date and complete. We believe that such reliance on the data for other purposes, particularly under an Open Banking regime, is both foreseeable and highly likely.

The question is one that relates to remoteness and the legal causation arising from a breach of contract and/or duty, which may be compensated by a damages award. Factual causation, as described above – ie the bank's poor data collection and maintenance processes without informing customers of these practices, have led to reliance by a customer to provide this information to a third party who subsequently acts honestly, but leads to a loss. We do not believe that the damage is too remote in this scenario.

[23] p. 67, *Review into Open Banking: Giving customers choice, convenience and confidence*, December 2017, https://static.treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open-Banking-_For-web-1.pdf

Under contract, the test is one of foreseeability[24] that is the loss will only be recoverable if it was in the contemplation of the bank. The loss must be foreseeable not merely as being possible, but as being not unlikely.

Under tort, the test for remoteness of damage is whether the kind of damage suffered was reasonably foreseeable by the bank at the time of the breach of duty.[25] The bank will be liable for any type of damage which is reasonably foreseeable as liable to happen even in unusual cases unless the risk is so small that a reasonable man would in the whole circumstances feel justified in neglecting it.[26]

There is also a banking law principle where the financial institution requires the mandate of its customer to validly debit an account. Only in exceptional circumstances can a customer be held liable for unauthorised transactions on their account. While Open Banking is read-access not write-access, the same principle might be instructive.

We believe that at the very least there is an arguable case that the bank's negligence has led to the loss and that this negligence is not so remote and unforeseeable as to be unreasonable.

The suggested result in the Report overwhelmingly benefits the bank data holder who is obliged to maintain proper data records, and leaves the consumer out to dry. If, as the Report claims, the aim of the regime is to build trust and confidence in the system, this liability regime as proposed will lead to its inevitable failure. If it were to go ahead, it will give consumers significant pause from proceeding to use an open banking product or service. Our organisations would also need to advise consumers of this clear risk. This result is not in the best interests of either potential data recipient FinTechs, nor is it in the interest of consumers.

We strongly believe that the liability principles put forward in the Report must be re-considered to ensure consumers are protected from the foreseeable negligence of data holders not keeping accurate, complete and up to date data records.

Recommendation

48. The Report needs to consider the risk and liabilities that may arise from the on-sale or provision of a customer's data. We believe that third party data recipients must be held liable for any sale to fourth parties where it is reasonably foreseeable that a loss or breach of the Open Banking regime laws and regulations may occur. One solution that needs to be considered is requiring accredited entities from only selling or sharing data to fourth parties who adhere to the accreditation criteria themselves.

[24] As traditionally set out in *Hadley v Baxendale ([1854] 9 Ex 341*

[25] *Overseas Tankship (UK) Ltd v Morts Dock and Engineering Co Ltd (The Wagon Mound No 1) [1961] AC 388*

[26] *Heron II [1969] 1 AC 350*

49. The liability principles put forward in the Report must be re-considered to ensure consumers are protected from the foreseeable negligence of data holders not keeping accurate, complete and up to date data records.

Chapter 5 – The data transfer mechanism

Recommendation 5.1 – application programming interfaces

Consumer representatives support the development of a dedicated application programming interface. We note however that the Report has stated that:

> *Open Banking should not prohibit or endorse 'screenscraping', but should aim to make this practice redundant by facilitating a more efficient data transfer mechanism.*[27]

While this seems pragmatic and a good compromise on its face, it does not take into account that the practice is highly likely to continue, now and after the introduction of an Open Banking regime – particularly by unscrupulous operators dealing with less knowledgeable, financially vulnerable consumers. And if it does continue there will also continue to be no protections in place for consumers misled into this form of information gathering and the subsequent loss of rights and other risks as detailed in the Report.[28]

We note too that it has been recently announced that FinTech's in Europe will be banned from using screen-scraping technology software to 'scrape' data held by banks to provide services to their customers under new PSD2 regulatory technical standards.[29]

We believe that the Open Banking regime will be a more successful one if the practice of screen-scraping is outlawed altogether.

Recommendation

50. The practice of screen scraping with respect to financial information should be outlawed.

[27] p. x

[28] At p.73, "*These 'screen scraping' or 'direct access' approaches are problematic because they:*

- *give the third party full access to the user's account, including potential to execute transactions*
- *require the third party to store the passwords, which can be a hacking risk*
- *are costly to develop as they must be reverse engineered rather than being designed to access a dedicated interface*
- *expose the customer to risk, as providing their login credentials to a third party is usually in breach of a bank's terms of service, and*
- *will stop working if a bank changes the way it presents its information.*

[29] Commission Delegated Regulation Supplementing Directive 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication, 27 November 2017, http://ec.europa.eu/finance/docs/level-2-measures/psd2-rts-2017-7782_en.pdf

Recommendation 5.2 starting point for the data transfer standards and Recommendation 5.3 - extensibility

Consumer representatives support the recommendations to use as a starting point for the Standards for the data transfer mechanism the UK Open Banking technical specification, as long as they remain in line with the EU PSD2 regulatory technical standard for authentication and communications, which provide a solid principles based framework from which to be guided. This is important to note given the potential for British policy development to shift away from EU frameworks from March 2019, ie "post-Brexit".

Consumer representatives also support the principle of developing core requirements with extensibility for future functionality.

Recommendation

51. The UK Open Banking technical specification should be used as the basis for standards for the data transfer mechanism, in line with the EU PSD2 regulatory technical standard for authentication and communications.

52. Extensibility should be built into the standards to ensure future functionality.

Recommendation 5.4 – customer-friendly authentication and authorisation

As indicated a number of times, consumer representatives are not as concerned as FinTech companies, with some friction being built into a system, particularly if it assists with greater security. While the UK Open Banking authorisation and authentication re-direct model is more streamlined, it is more vulnerable to phishing, as the Report highlights.

We believe that consumers are becoming more and more used to, even have come to expect and want , multi-factor authentication[30] and two step verification[31], as awareness of the risks and security flaws inherent in online transactions increases. While multi-factor authentication is not foolproof[32], it is safer than the redirect method.

We believe it may be more prudent to support a de-coupled approach as a starting point rather than the UK model but are not averse to further investigation and consideration of all models to ensure the highest level of security for consumers.

---

[30] Where two or more pieces of evidence are used to authenticate an identity.

[31] Where a user's identity is verified by utilising something they know (a password say) and another step than involves something there have via another mechanism say a 6 digit number randomly generated from a service provider.

[32] For example, see Ian Thompson, After years of warnings, mobile network hackers exploit SS7 flaws to drain bank accounts, *The Register*, 3 May 2017, https://www.theregister.co.uk/2017/05/03/hackers_fire_up_ss7_flaw/

Finally we believe that, similar to the approach to consent, it is prudent for the Data Standards Body in developing the authentication and authorisation standards and process consumer test the standards before settling on a final version. Involvement of the Behavioural Economics team of ASIC again is essential.

Recommendation

53. A de-coupled approach as a starting point may be more prudent rather than the UK's redirect-based authorisation and authentication model but are not averse to further investigation and consideration of all models to ensure the highest level of security for consumers.

54. In developing the authentication and authorisation standards and process, the Data Standards Body should consumer test the API before settling on a final version. Involvement of the Behavioural Economics team of ASIC again is essential.

Recommendation 5.6 – persistent authorisation

Consumer Representatives generally support the concept of persistent authorisation as this should be time bound and not perpetual. We support the consumer being able to:

a) limit the authorisation period of their own choosing;

b) be able to do so at any time, at their own discretion;

c) revoke authorisation through the third party or via the bank data holder

d) be notified periodically that they are still sharing information;

e) have the authorisation expire after a set period.

Recommendation

55. Consumers should be able to:

a) limit the authorisation period of their own choosing;

b) be able to do so at any time, at their own discretion;

c) revoke authorisation through the third party or via the bank data holder

d) be notified periodically that they are still sharing information;

e) have the authorisation expire after a set period..

Recommendation 5.9 – access without online banking

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

Consequently we do support providing access to Open Banking to those without online banking access, but would want to see further protection and security measures here to avoid potential elder abuse, misuse or other unscrupulous behaviour.

Recommendation

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

Recommendation 5.10 – transparency

Consumer representatives agree that customers should be able to access a record of their usage history and data holders should keep records of the performance of their API that can be supplied to the regulator as needed.

Recommendation

57. Consumer representatives support Recommendation 5.10

Chapter 6 – Implementation and beyond

Recommendation 6.4 – consumer education programme

Consumer representatives support the ACCC coordinating the development and implementation of a timely consumer education programme for Open Banking. Participants, industry groups and consumer advocacy groups should lead and participate, as appropriate, in consumer awareness and education activities.

We reiterate our misgivings that consumer behaviour research has long demonstrated, that there are limits to the role education and disclosure regimes can play. A reliance on mere disclosure, education and financial literacy programs will not avoid consumer harms.

This is not to argue that it shouldn't take place, but that strong consumer protections need to be built into a system to ensure there is less potential for exploitation of consumer interests.

Recommendation

58. Consumer representatives support Recommendation 6.4

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) 9212 4216.