OPEN BANKING REVIEW

RESPONSE TO ISSUES PAPER

September 2017

Public

CONTENTS

Executive Summary 3
Purpose of open banking 5
What is open banking? 5
Why open banking? 5
Principles for open banking 7
Suggested rationales for open banking 8

Consumer use cases – Data requirements 9
Introduction 9
Data sets needed and data form 13
Transfer mechanism 17
Frequency 19
Product scope 19
Data transferors 20
Consumers 20

Data Risk 22
Introduction 22
Risk assessment 22
Risk mitigants 24

Use case assessment 26
Legal Reforms 28
Introduction 28
Mandated availability 28
Clarify the liability of data transferor 29
Set up an appropriate regulatory framework 31
A new data-related act 32

Regulatory model 33
Introduction 33
Oversight of open banking 33
Data transferors 34
Data recipients 35

Competition 39
Introduction 39
Charging for the transfer of data 39
Economy-wide open data as end-state 40
Clear limitations on use 40
Standardisation of data 40

EXECUTIVE SUMMARY

1. ANZ appreciates the opportunity to make a submission to the Open Banking Review.

2. As we have previously stated, we support consumers across all sectors of the economy, including banking, having greater access to their data.[1] Consumers will benefit from open data, including through understanding their own behaviour and comparing products and services. Working out which bank offers the best deposit account will be easier for consumers when they can use data about their past account usage and a comparison site's algorithm.

3. We believe that open banking should be approached as a consumer-focused pathway to economy-wide open data, as recommended by the Productivity Commission in its March 2017 report. As Australia moves towards open data, open banking is a valuable opportunity both to learn how consumers can use their data and to start putting in place the frameworks needed to keep data secure across the economy.

4. In anticipation that the window between the start of open banking and the start of economy-wide open data will be relatively short (perhaps one or two years), the initial phase of open banking should be simple and quick to implement without undue risk to consumers. We would then see this initial phase of open banking being subsumed by economy-wide open data. That said, we think that the bones of the legal and regulatory framework needed for economy-wide open data should be implemented now to support open banking. This is to ensure that open banking is safe from day one.

5. As such, we recommend that this initial phase of open banking should:

    - Facilitate specific and straightforward consumer 'use cases' that will help consumers compare products (both in a generic and personalised way) and gain a basic understanding of their banking activity

    - To enable these use cases, involve banks opening up the following data sets:

        - Product attribute data concerning simple deposit products that are made available by public application programming interfaces (APIs); and

        - Transaction data drawn from deposit products in summarised form that are made available, with customer consent, by either secure file transfer or permissioned APIs

    - Be underpinned by a new 'Data Act' that establishes a framework for mandating open data through the economy (with banking the initial mandated sector), closes gaps in the *Privacy Act 1988* (Cth) and establishes a regulatory and liability framework that

[1] Letter from Mr Shayne Elliott to Mr David Coleman MP, Chair of House of Representatives Standing Committee on Economics (6 March 2017); available at: http://www.aph.gov.au/~/media/02%20Parliamentary%20Business/24%20Committees/243%20Reps%20Committees/Economics/Review%20of%20the%20Reserve%20Bank%20second%20report/Documents/ANZ%20response%20to%20recs%20for%20web.pdf?la=en

is ready to support economy-wide open data (subject to any learnings from open banking)

6. This is a deliberately simple and safe form of open banking. We expect implementing banking-specific and then economy-wide open data in a safe way to be complex and challenging. While some banks may be ready to implement open data on a stand-alone basis, achieving industry-wide standards for data sharing and a regulatory framework that underpins consumer trust in data availability will take deliberation, effort and law reform. We would suggest that our simple form of open banking is an appropriate initiation point for economy-wide open data. Once economy-wide open data is implemented, and subject to its final form, a wider range of data and use cases would be available.

7. This initial phase of open banking could be implemented with relative speed. This will allow time to learn before economy-wide open data is implemented. We would suggest the following timetable may be appropriate:

    - Pass a new 'Data Act' in the first half of 2018
    - Implement a regulatory framework through the middle of 2018 after the passage of the new 'Data Act'
    - Government, industry and consumer groups to simultaneously work on data format and security standards
    - Target commencement of open banking for the end of 2018 with possible phasing by data transferor (large then small banks) and data type (product attribute data then summarised transaction data)
    - Target economy-wide open data for the end of 2019

8. To explain these recommendations, this paper is structured as follows:

    - First, we set out why open banking should be pursued
    - Second, we look at possible consumer use cases and the data needed to enable them
    - Third, we look at the data risk associated with the data sets and transfer mechanisms that are needed for the use cases
    - Fourth, we bring the preceding two chapters together to offer an implementation recommendation concerning which use cases and data sets should be pursued
    - Fifth, we explore the legal reforms needed to enable these use cases within open banking
    - Sixth, we posit possible regulatory frameworks that might underpin open banking
    - Last, we offer some suggestions on keeping open banking competitively neutral

PURPOSE OF OPEN BANKING

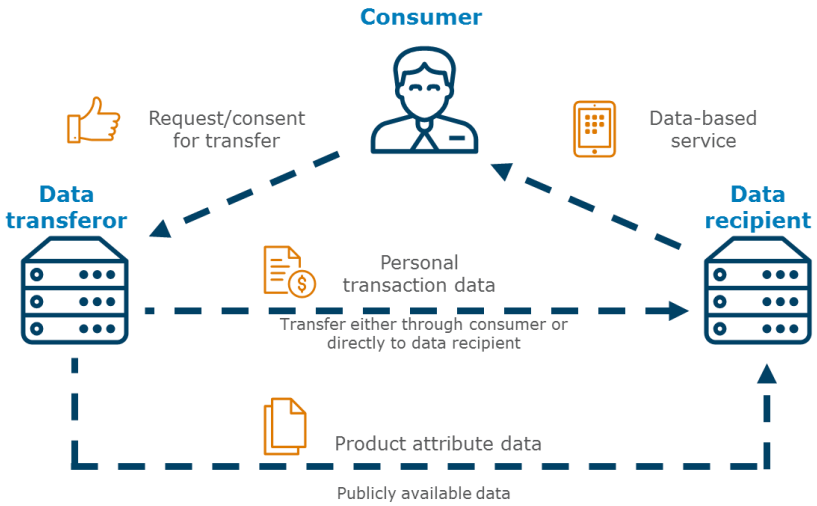
Key points

Open banking should have two rationales:

- **First, open banking should be directed primarily towards helping consumers make better decisions and manage their finances more effectively**
- **Second, open banking should be used as a pathway towards economy-wide open data**

What is open banking?

1. Open banking would involve the transfer of data held by banks (**data transferors**) to third parties (**data recipients**) to allow the data recipient to provide a service to a mutual customer (the **consumer**). Some of this data could concern the products offered by the bank (**product attribute data**). Some of it could relate specifically to the consumer, such as their transaction history and account balances (**transaction data**). This basic idea is set out in the diagram below.



Why open banking?

The opportunity

2. Data is powerful. With the help of modern algorithms, it helps organisations understand human behaviour. Businesses, including banks and other financial services firms, use it to assess a borrower's likelihood of repaying loans, financial position and goals and purchasing preferences. Consumers can also use data to understand their own behaviour and interests. Empowering consumers to make better decisions is appealing both to help protect consumers' interests and to drive more robust competition.

3. For example, with the help of an algorithm, consumers could use product attribute data and their personal bank data to assess what financial product will best suit their needs. This may help overcome the decisional challenges that consumers face when selecting financial services. These challenges include needing to comprehend lengthy terms and conditions, being able to conceptualise from terms and conditions the possible utility from the product and forecasting its likely costs. Algorithms could use historical behaviour (as

embedded in the personal bank data) to predict future benefit (by feeding that personal bank data through the product attribute data). Product *use* disclosure could be more helpful to consumers than product *attribute* disclosure alone.[2]

4. The potential for data to help consumers was recognised by the Productivity Commission in its report on *Data Availability and Use*.[3] In that report, the Commission recommended that consumers have a 'comprehensive right' to their data. Among this right's many components would be the ability for consumers to request and direct the transfer of their data from a data transferor to a third party. This right would enable consumers to leverage the power of their data from across the economy. **Economy-wide open data** could see consumers empowered to exercise better choices in areas such as telecommunications, energy, social media, consumer goods as well as financial services.[4]

5. Greater bank data availability could also help drive innovation. Service providers may develop innovative ways of understanding and improving financial behaviour and outcomes. Of course, because data is valuable, open banking could underpin the business models and practices of new and existing firms. Being able to use the data that others have collected would clearly lower barriers to entry for a range of actors, large and small. In doing this, though, the transfer of data from one competitor to another (at the consumer's request) could see a basis of commercial advantage shifted, potentially without a corresponding value transfer.

The challenges

6. However, the ability of open data to help consumers and change markets is largely unproven in praxis. For example, in the UK where open banking is the most advanced, research by Accenture Payments concerning the attitudes of UK consumers indicates about 70% prefer to trust a bank with their data.[5] This indicates that the propensity of consumers to share data outside of banks may be relatively low. In Australia, the Australian Energy Market Commission is still observing issues with consumer switching and use of official government comparator sites in the energy markets despite mandating data availability since December 2014.[6] As of July 2017, it notes that data availability may still drive change and innovation.[7]

7. Further, as discussed below, open banking would potentially involve the dissemination of personal bank data through actors that sit outside the regulated banking environment. This means that bank-level data security requirements may not apply to data that consumers have hitherto trusted as secure. Recent IT system compromises, such as the one affecting Equifax, highlight modern data security risks.[8] Compromised personal bank data could expose consumers to identity theft and privacy concerns. As evidence of

---

[2] See Oren Bar-Gill and Oliver Board "Product Use Information and the Limits of Voluntary Disclosure" (2010, Paper 239) *New York University Law and Economics Working Papers.*
[3] Productivity Commission *Data Availability and Use* (31 March 2017).
[4] Consumers already have the right to access and transfer their energy data. Australian Energy Market Commission *Customer access to information about their energy consumption* (November 2014).
[5] Accenture Payments *Consumers' initial reactions to the new services enabled by PSD2*
[6] See Australian Energy Market Commission *2017 AEMC Retail Energy Competition Review*(25 July 2017),ii; available at: http://www.aemc.gov.au/getattachment/006ad951-7c42-4058-9724-51fe114cabb6/Final-Report.aspx.
[7] Ibid, 139.
[8] https://mobile.nytimes.com/2017/09/08/technology/seriously-equifax-why-the-credit-agencys-breach-means-regulation-is-needed.html?referer=https://t.co/3qfphFpmJT?amp=1

consumer concern about data security, research in connection with the UK open banking standard work indicates that 77% of consumers 'believe that third parties accessing their financial data should be regulated'.[9] While this issue is soluble, it should be approached cautiously to ensure consumer faith in the safekeeping of their data is not undermined. A robust regulatory framework is necessary.

Principles for open banking

8. Open banking, then, offers (as-yet unproven) hopes for consumer empowerment coupled with some (soluble) data security risks. Further, there are many different paths that Australia could take to implement open banking. Across the dimensions of how consumers could benefit from open banking (the use cases), the data sets that should be opened up, mechanisms for transmitting the data and possible regulatory frameworks, there are many permutations for open banking.

9. Because of this, we think it is important to identify the principles that should guide the policy design. These principles are intended to be the values that help us pick the right permutation for open banking. For us, these principles would be the following.

The consumer must be the focus of open banking

The interests and objectives of consumers should be the lodestar of open banking. A consumer's data should be made available to help that consumer make better choices and manage their money more effectively.

The data security risks of open banking need to be managed

To work, consumers need to trust open banking, and open data more broadly. A person's bank data can be used to steal their identity and to reveal their preferences, habits and locations. This risk exists today. However, open banking could accelerate the risk through the dissemination of bank data to a broader range of data holders. This risk is surmountable with careful consideration. It will need to be calibrated with the imperative that risk management obligations on data recipients should be reasonable (i.e. no insurmountable barriers to entry).

Open banking should not create competitive imbalances

Data is valuable. To collect it, organise it, store it and protect it takes money and effort. The insights from data drive modern businesses. While open banking can catalyse competition by empowering consumers and fostering innovation, it should not be used to transfer resources from one sector of the economy to another at no value. Charging structures for data transfers will need to balance commercial interests and consumer entitlements.

---

[9] *The Open Banking Standard*, 16, available at: https://www.paymentsforum.uk/sites/default/files/documents/Background%20Document%20No.%202%20-%20The%20Open%20Banking%20Standard%20-%20Full%20Report.pdf

Economy-wide open data should be the end-state of open banking

The Productivity Commission's proposal for consumers to have a comprehensive right to access and transfer data relating to them held by others is a powerful one. It has the potential to transform the Australian economy. Open banking should be used as a short-term pathway towards safe economy-wide open data.

Suggested rationales for open banking

10. With these principles in mind, we would recommend that open banking be pursued for two reasons.

11. **First, open banking should be directed primarily towards helping consumers make better decisions and manage their finances more effectively**. Given the data relate to consumers, they should be the main beneficiaries of its availability. We set out below a number of use cases that are aimed at these outcomes.

12. **Second, open banking should be used as a pathway towards economy-wide open data.** This learning would be valuable as the Government finalises the framework for economy-wide open data. It would supplement learnings that can be drawn from the energy sector about the utility of open data.

13. For completeness, we note that we understand open banking (and economy-wide open data) to only involve 'read' access to the data, not 'write' access (ie the ability of a third party to amend data within the data transferor's system). The New Payments Platform (**NPP**) will provide a number of access options to potential payment service providers. These providers include overlay service providers that are able to sit on top of the NPP infrastructure and use other institutions' bank accounts. Subject to the resolution of security, authentication and fraud concerns, this may eventually include directing the payment of amounts from those bank accounts to other accounts. Such functionality would significantly increase innovation and competition in payments. We would suggest that the NPP form the basis of competition in payments rather than a new regime concerning write access to accounts.

CONSUMER USE CASES – DATA REQUIREMENTS

Key points

The consumer use cases with the lowest data complexity are:

- **Generic comparisons of products/services**
- **Personalised comparisons of products/services**
- **Basic financial management (point-in-time analysis of a consumer's financial position on limited dimensions)**

These use cases could be facilitated using product attribute data delivered through public APIs and summary transaction data delivered through either direct transfer of a CSV file to a data recipient or permissioned API.

The simplest products to provide the use cases over are deposit products (savings and transactions accounts).

Other data sets (such as complete transaction data) and bank products (such as credit cards) carry greater data complexity. Such complexity could push out the implementation timeframe and, as discussed in the next chapter, carry greater risk.

Introduction

Focus on consumer use outcomes

14. If the primary purpose of open banking is to help consumers, it is important to consider how consumers could use open bank data. This will drive what data should be opened up. The Productivity Commission recommended a broad definition of 'consumer data' that would be transferable under the economy-wide comprehensive right. However, it recognised that this definition should be driven by 'outcome' – '…that which is sufficient to afford consumers greater choice in services and spur competitive pressures…'.[10]

15. As Australia starts to explore open data, we think it would be useful to start with opening data that is tailored to achieving specific outcomes. This will allow the Government, industry and consumers to learn what does and does not work.

16. Set out below are a range of salient consumer use cases that a data recipient could offer in an open banking environment. They highlight the different forms of data that may be needed, the potential transfer mechanisms and the issues concerning data recipients. By considering these dimensions, we can consider the data complexity bound up with each use case.

[10] Productivity Commission, above n 3, 200.

POSSIBLE CONSUMER USE CASES

Use case	Example
Generic comparison	**Which bank or financial institution offers the lowest fees and/or interest rate?** Consumers could compare fees and interest rates across bank products and services. The comparison would not take into account the consumer's individual circumstances
Personalised comparison	**Which product/service might best meet my needs?** Consumers could use data concerning their individual circumstances to identify the product or service that might best meet the consumer's specific needs (ie product use disclosure)
Basic financial management	**How can I save more money?** Consumers could use point-in-time data concerning their income and expenses to identify ways of saving more money
Complex financial management	**What is my detailed financial position on a real-time basis?** Consumers could use real-time data concerning their income, expenses and exposures to continuously understand their financial position in detail (e.g. categories of spending, benefit of offset account on mortgage, projected savings/deficits)
Apply for credit	**I need to evidence my capacity to repay** Consumers could use point-in-time data concerning their income and expenses to support an application for a loan

17. These uses all require different data sets and means of transferring the data sets to third parties. Further, there are the issues of which bank products and services are covered, which consumers should be able to access their data and which data recipients can receive the data. As the data sets and data recipients change, the data complexity also changes. The table below sets out the data permutations possible for the use cases.

Excluded use cases

18. Of course, other consumer uses are possible. Use cases that have not been analysed in detail include know-your-customer (KYC) assessments, account switching and consumer purchasing propensity analysis.

19. We have excluded these use cases from our consideration for a range of reasons.

20. Consumer purchasing propensity analysis is primarily about helping firms offer services to consumers rather than helping consumers engage with their banking. As such it does not meet our principle of the consumer being the focus of open banking.

21. On switching, it is not clear that this would be made easier by open banking. The main difficulty with switching is the identification and transfer of recurring payments, particularly from credit cards. Banks do not always have the data necessary to identify these payments. Thus, data availability may not solve this residual impediment to

switching. Instead, we note that reforms to the Code of Banking Practice and innovations like digital identity may offer more hope in facilitating switching.[11]

22. It is conceivable that KYC data could support switching to a limited degree. Banks could be required to transfer data that they have relied upon to establish and verify the identity of consumers to a data recipient that the consumer wished to open a new account with.

23. However, this transfer would not solve the KYC challenge for the data recipient. The transferred data may be dated and not suitable for a fresh KYC assessment. It would not absolve the data recipient from their obligation to establish and verify the identity of and otherwise risk-assess the consumer. KYC obligations can be bank- and product-specific. Critically, an originally erroneous KYC assessment could be perpetuated through the system. The data sets involved in KYC also lie at the high end of the risk spectrum. Further, the transfer of KYC assessments could involve the transfer of 'derived' data to a competitor. Thus, we do not think that the KYC use case can be properly met with open banking. Again, Government may like to consider alternative solutions such as digital identity for this issue.

[11] http://www.bankers.asn.au/consumers/code-of-banking-practice/

USE CASE AND DATA REQUIREMENT PERMUTATIONS

Use case	Data set needed	Data form	Transfer mechanism	Frequency	Product scope	Data transferors
Generic comparison 	**Product/service attribute data** Data concerning products and services	**Industry standardised** Data needs to be formatted to industry-level standard to allow comparison sites to ingest it from multiple providers	**Public API**	**Always available, updated as product terms and conditions change**	**Product-by-product basis**	**All providers of product/service in market**
Personalised comparison 	**As above** **+** **Consumer's transaction data**	**As above** **+** **Summary of transaction data** Use case could be met with summary of data fields relevant to comparison eg for deposit accounts, total fees paid and deposits made per month **or** **Complete transaction data** The consumer's complete statement data could be delivered	**As above** **+** **Download CSV file of transaction data** Consumer could download a CSV file with transaction data (either summary or complete) and email it to comparison site **or** **Transmit CSV file of transaction data** Bank could send CSV file to data recipient at consumer's request via secure file transfer protocol **or** **Permissioned API** Bank could make data available via permissioned API	**As above** **+** **Provide consumer's transaction data when requested by consumer (ie one-off pull requests)**	**As above**	**As above** **+** **For the consumer's transaction data, comparisons could be based on data drawn from one or more the consumer's banks or other financial institution** For consumers who have accounts with multiple institutions, some use cases will require data from them all. For example, if a consumer has a mortgage with one bank and their transaction account with another, then a mortgage comparison that needs an understanding of capacity to repay may require data from both
Basic financial management 	**Consumer's transaction data**	**As above** (for consumer's transaction data)	**As above** (for consumer's transaction data)	**As above** (for consumer's transaction data)	**As above**	**As above** (for consumer's transaction data)
Complex financial management (real time) + apply for credit  	**Consumer's transaction data**	**Complete transaction data** The consumer's complete statement data could be delivered	**Permissioned API** Bank could make data available via permissioned API	**Continuous** (one off for 'apply for credit')	**All products that the customer holds**	**All banks and other financial institutions that the consumer has a relationship with**

Data sets needed and data form

24. The use cases identified would require two basic types of data:

    - Product attribute data; and
    - Consumer's transaction data.

25. This data could be presented in different ways. The data form concerns how the data is organised as it is made available to third parties or consumers.

Product attribute data

26. Product attribute data is data that concerns the terms and conditions of financial services and products.[12] In the table below, we have set out the indicative data fields for a range of common bank products. These are the data fields that are required to describe the terms and features of the products. In order to be usable by comparison sites, these data fields would need to be standardised.

27. As is clear, the data complexity of products varies. This occurs both on the number of variations of products within a product category and the data fields for the product. Credit cards, for example, include multiple card types (e.g. low rate, reward, low fee) and have significantly more features than deposit products (e.g. reward structures, interest free periods, insurance). With an increase in data fields, the work involved in agreeing the standardisation would also increase.

28. Further, some products are only offered by authorised deposit-taking institutions while others are offered by non-bank providers as well. The greater the number of institutions offering a product, the more stakeholders involved in the standardisation of the data fields. For example, transaction and savings accounts have a, *prima facie*, low data complexity because not only do they have low data field counts, but they are only offered by authorised deposit-taking institutions. In contrast, credit cards not only have a large number of data fields but can also be offered by any institution with an Australian credit licence. This gives cards a high data complexity.

29. We note that the standardisation of fields may inhibit competition if banks were unable to add new features to their products and services without these being reflected in a standardised data field. In addition to increasing the product development costs, if banks were mandated to provide data on all features of their products, it would also give their competitors the chance to copy the product feature before release.

---

[12] See Article 12.1.2 of the Competition and Markets Authority *The Retail Banking Market Investigation Order 2017* for the UK articulation of this data set.

PRODUCT TAXONOMY AND INDICATIVE ATTRIBUTE DATA FIELDS

Product category	ANZ product sets	Indicative attribute data fields for standardisation		Institutions offering (potential data transferors)	Estimated data complexity
Transaction accounts (deposit) 	• Access Advantage • Access Basic • Pensioner Advantage	• Account Service Fee • Interest Rate • Minimum Balance • Transactions per month • Additional Transactions fee • ATM Fee	• Overseas Transaction Fee • Overseas ATM Fee • Dishonour Fee • Overdrawn Fee • Non-Payment Fee • Eligibility	Authorised deposit-taking institutions	**Lower** Few data fields and only offered by ADIs
Savings accounts (deposit) 	• Online Saver • Progress Saver • Premium Cash Management	• Account Service Fee • Interest Rate • Minimum Balance • Transactions per month • Additional Transactions fee • ATM Fee	• Overseas Transaction Fee • Overseas ATM Fee • Dishonour Fee • Overdrawn Fee • Non-Payment Fee • Eligibility	Authorised deposit-taking institutions	**Lower** Few data fields and only offered by ADIs
Term deposit (deposit) 	• Advance Notice Term Deposit • Term Deposit	• Term • Interest Rate • Minimum Amount		Authorised deposit-taking institutions	**Lower** Few data fields and only offered by ADIs
Offset accounts (deposit) 	• One • Equity Manager	• Account Service Fee • Minimum Balance • Transactions per month • Additional Transactions fee		Authorised deposit-taking institutions	**Lower** Few data fields and only offered by ADIs
Personal loans 	• Variable Rate Loan • Fixed Rate Loan • Secured Car Loan	• Interest Rate • Minimum Loan Amount • Maximum Loan Amount • Loan Approval Fee - Establishment • Loan Administration Fee – Ongoing • Minimum Loan Term • Maximum Loan Term	• Late Payment Fee • Early Termination Fee • Administrative Default Fee • Redraw (f) • Exit Fee (f) • Eligibility	Australian credit licence holders	**Medium** Multiple potential data transferors
Home loans 	• Standard Variable HL • Fixed HL • Equity Manager (LoC) • Simplicity PLUS HL • Land Loan • Supplementary Loan	• Interest Rate • Interest Type • Minimum Loan Amount • Maximum Loan Amount • Maximum Loan Term • Fixed Rate Loan Terms • Repayment Type • Repayment Frequency	• Early Repayment Cost • Redraw Fee • Lenders Mortgage Insurance • Loan Approval Fee - Establishment • Loan Administration Fee - Ongoing • Renegotiation Fee • Lock Rate Fee • Property Type (Res or Inv)	Australian credit licence holders	**Medium** Multiple products and potential data transferors
Overdrafts 	• Assured • Personal Overdraft	• Interest Rate • Approval Fee • Credit Facility Fee		Australian credit licence holders	**Medium** Multiple potential data transferors

Product category	ANZ product sets	Indicative attribute data fields for standardisation	Institutions offering (potential data transferors)	Estimated data complexity
Credit cards VISA	• AFF Classic • AFF Platinum • AFF Black • ANZ Rewards • ANZ Rewards Platinum • ANZ Rewards Black • ANZ Travel Adventures • ANZ Travel Card • ANZ Low Rate • ANZ Low Rate Platinum • ANZ First • ANZ Platinum	Rates and fees • Total Account Fee • Annual Account Fee • Annual Rewards Fee • Interest Free Days • Purchase Rate • Cash Rate • Add. Cardholder Fee • Min Monthly Repayment • Min Credit Limit • Card Issue Fee • Initial Load Fee • Reload Fee • Replace Fee • CCY Conversion Fee • Int. ATM Withdrawal Fee • Inactivity Fee • BT Revert Rate • BT Fee • Over Limit Fee • Late Payment Fee • Balance Transfer Fee Points Earn Rate • Earn Rate • Direct Earn • Points Cap • Qantas Bonus Pts Points Redempt. & Spend • Pts Redemption Flight • Pts Redemption Gift • Pts Spend Flight • Pts Spend Gift Travel Feature • Travel Insurance • Overseas Travel Insurance • Overseas Medical Insurance • Other Insurances • Overseas transaction fees • International Spend • Comp QFF Membership • Comp Lounge Passes • Lounge Access • Other benefits • Misc (Other) • Warranties • Rental Excess Cover • Personal Concierge /Bonus Points Mall Other • Misc • Warranties • Personal Customer Assist Line/Service • Visa/AMEX Bespoke Event • Scheme • App/IB • Loyalty • Currencies • Load / Reload options • Spare Card	Australian credit licence holders	**High** Multiple products, data fields and potential data transferors

Transaction data

30. Transaction data concerns the credits, debits and balances of a loan, deposit or credit card account. Depending on the product type, this would capture any interest paid to or from the consumer, any fees they may incur, any loan repayments as well as the amounts they spend from the account and income received into it. This kind of data is already captured and made available to consumers through statements.

31. We note that there is the issue of how much transaction data should be transferable (ie how many years). Most banks make available 1-2 years of transaction data already. The quantum of data needed would depend on the use case although we suspect most use cases could be supported with 1-2 years of data.

Summarised transaction data

32. The use cases proposed above do not all need the full details that are presented in statements. Both the use case of personalised comparisons and basic financial management could be fulfilled with summarised transaction details. Data transferors could collect and deliver standardised packets of summarised data to underpin specific use cases rather than entire transaction histories. As discussed below, this would have data security benefits as summarised transaction data could be safer to share than complete transaction data (although it could still disclose sensitive information).

33. For example:

- Personalised comparisons of mortgage

  This type of comparison would need the consumer's outstanding loan principal, current interest rate, monthly repayment history and potentially any uncommitted monthly income (together with the property value) (these last two values may be proprietary to specific banks)

- Personalised comparisons of credit card

  This type of comparison would need the consumer's average outstanding balance (split into purchases, cash advance and, potentially, balance transfers), monthly interest paid, monthly repayment history and potentially points collected

- Basic financial management

  To show whether a consumer was meeting a savings goal each month, summarised data concerning their monthly income and expenses could be delivered

Complete transaction data

34. Complete transaction data refers to the full set of transaction data that constitutes a consumer's statement of account. Some consumer use cases could only be provided with

this full set of data. For example, complex financial management would require granular data on the consumer's financial position and activities.

Excluded data

Derived data

35. None of the use cases identified above needs data that is proprietary to, or which has been subject to manipulation and analysis by, the data transferor (so-called 'derived' data). The transaction data that could support the use cases above is that which is already presented to consumers in the form of their statements.

36. While it is possible to imagine use cases that would benefit from derived data (for example the data recipient offering credit products based on a data transferor's credit scoring), this would raise both competition and legal liability issues. Derived data reflects competitive effort and is used by firms and banks to differentiate themselves from others. The forced transfer of this from one firm to another would erode a basis of competition. Further, it would involve the reliance of data recipients on the data analysis of the data transferor (eg using the latter's credit scores). This could involve liability issues if the data recipient suffered loss due to the data or a consumer felt prejudiced by it.

37. The exclusion of derived data from open banking would be consistent with the Productivity Commission's recommendation concerning the data covered by the economy-wide comprehensive right.[13] The Commission recognised that 'imputed' data may not be appropriately caught by the comprehensive right. For banks, this included 'likelihood of a person having difficulty repaying their debt based on characteristics that could be ascribed to them'.[14]

Paper-based data

38. The commission similarly recognised that the comprehensive right would only capture digital data.[15] Thus, firms would not have an obligation to hand over, or digitise, data stored in paper form. A similar limitation on the data transferable under open banking would be appropriate.

Transfer mechanism

39. There are four basic transfer mechanisms that could be used to send the data from the data transferor to the data recipient. These are arranged below from simplest to most complex. We note that other transfer mechanisms could be possible, including a dedicated 'pipe' or blockchain. However, those other mechanisms may not be scalable to a large number of recipients (eg a 'pipe' from data transferor to recipient) or may take substantial effort to establish (eg blockchain).

---

[13] Productivity Commission, above n 3, 207.
[14] Ibid.
[15] Ibid, 204.

40. While these are the transfer mechanisms that currently seem suitable today, we note that innovation may mean that more apt transfer mechanisms are developed in the future. Open banking should allow the adoption of such mechanisms as and when appropriate.

Download CSV file of transaction data

41. The simplest way of getting transaction data to consumers is to allow them to download a CSV file of their transaction data from their secure internet banking portal. Many banks already allow their customers to do this. The customer could then send the file to a third party data recipient.

42. To enable open banking, the ability of consumers to download their data would likely need to be made clearer and simpler. Presently, the download option is typically part of the statement view function of internet banking portals. It may need to be made salient to ensure consumers are aware of their options.

43. This type of mechanism would support the use cases of personalised comparison and basic financial management. However, we note that CSV files are capable of manipulation. This may rule this method out of any use case that relies on the integrity of the data as recorded by the data transferor.

Transmit CSV file of transaction data

44. Instead of the consumer needing to download a file to their home computer, banks could amend their internet banking function to allow consumers to transmit the file to a third party data recipient. Once authorised by the consumer, the bank data transferor would send the file directly to the data recipient via secure file transfer protocol.

45. This mechanism could work with bank data transferor presenting consumers with a list of authorised data recipients. Below we recommend the regulatory framework include a registration mechanism whereby data recipients need to hold a licence. Banks could use this licence to know which data recipients are safe to list.

46. This option would remove the need for the consumer to do anything more than designate who they would like to receive their data. As discussed below under 'Data Security', it would also remove the risk that data is compromised while on the consumer's home computer or mistakenly sent to the wrong party by the consumer.

47. Again, this type of mechanism would support the use cases of personalised comparison and basic financial management.

Public API

48. A public application programming interface (**API**) would allow any entity to develop software that can access and download the data. The standards for the API would be publicly available. Third party developers could use those standards to write programs to access and then incorporate the data in their offerings.

49. This form of transfer mechanism would be suitable for data that does not concern consumers or is not otherwise commercial-in-confidence. Product attribute data, which is already made available via mandatory disclosure, could be delivered this way.

50. Public APIs would allow banks to continuously make their product attribute data available and update it as they see fit. This would enable both generic and personalised comparisons by allowing product/service comparison sites to display the current offerings from banks and others.

Permissioned API

51. APIs could be used to expose transaction data if they were structured to only allow authorised data recipients to access designated data packets.

52. In addition to the API, a system would be needed to accredit data recipients in respect of specific data packets from specific customers who have consented to the data recipient accessing the data. This issue of accreditation and consent is discussed below.

53. This form of mechanism would likely be necessary to enable complex financial management use cases that depend on real-time access to consumer bank data.

Frequency

54. The frequency with which data is available for transfer from data transferor to data recipient will be important for the cost of implementation.

55. Continuous availability would be needed for product attribute data to enable comparison services to operate.

56. Both personalised comparison and basic financial management services could be performed with one-off data transfers that are initiated by the consumer. Thus, when the consumer wanted to perform a comparison or understand their financial position, it could request that the data be transferred from data transferor to data recipient (or transfer the data itself). These use cases would not be dependent on continuous availability of data.

57. However, complex financial management services would likely rely on continuous data availability. We note that the Productivity Commission has rejected the idea of continuous availability: 'A request cannot create a constant stream of updated information from one party to another'.[16]

Product scope

58. Product scope refers to the use cases' requirements concerning the products they need data about. With the exception of complex financial management and credit applications, the use cases could be structured to address single products. For example, open banking

[16] Ibid, 221.

could enable generic comparisons of deposit products without needing to enable comparisons of mortgages or credit cards.

59. However, complex financial management or credit applications would need to be able to draw data from the consumer's entire product suite in order to understand their financial position. Thus, data concerning the consumer's transaction accounts, credit cards and loans would all need to be available to enliven such use cases.

Data transferors

60. A critical element of the success of the use cases is ensuring consumers have complete data sets available to them.

61. Australia has highly diverse and contestable mortgage, deposit and credit card markets. For example, there are about 100 mortgage providers in Australia, not all of which are banks. This means that if comparison sites are to present accurate pictures of the ranges of products available to consumers, then they need to be able to draw product attribute data from a broad range of providers.

62. If a provider were not to provide product attribute data, then a comparison site may not be able to present the provider's offerings to site viewers either at all or as easily as providers which do provide product attribute data. Making product attribute data available may then become a competitive requirement.

Consumers

63. The products that are listed above are all retail consumer products. While cognate products are also offered to small business customers, and open banking could be extended to such customers, most banks already make data available to small business customers through accounting software providers.

64. For example, ANZ's business customers are able to register so that automatic, direct bank feeds of transaction data are sent to customers' compatible accounting software packages. ANZ has set up direct bank feeds with a number of accounting software providers to make reconciling business accounts easier. This service is available at no cost to customers.

65. As such, while the change required to implement open banking for small business may not be great given the current state, this also means that there could be limited benefit in mandating open banking for such customers at this stage.

66. We acknowledge that the Productivity Commission recommended that the economy-wide Comprehensive Right be held by small businesses with a turnover of $3m per annum or less.[17] This would give them the right to transfer data. We note that articulating what

[17] Ibid, 198.

constitutes a ‘small business’ would need consultation given the various extant definitions across regulations and business practices.

DATA RISK

Key point

Product attribute data delivered through public APIs and summary transaction data through direct transfer of a CSV file to a data recipient or permissioned APIs are the safest forms of open banking.

Any residual risk should be managed through:

- Consent and authentication procedures for data recipients
- Data security and use standards for data recipients

Introduction

67. Consumer faith in data security will be necessary for open banking and open data more broadly. If consumers do not believe their data is secure when they share it, they will be unlikely to embrace data availability. The main risks with open banking concern identity theft, privacy breaches and misuse of data. Transaction data, including static account information, could support the illegal assumption of the data owner's identity. It could also be used to reveal personal attributes.

Risk assessment

68. The risk involved in making the data available to support each of the use cases depends on its sensitivity and the means of transfer.

69. Product attribute data has very low risk sensitivity. It is already publicly available and does not disclose any personal or commercial confidences. The key risk with this data is that it is altered (e.g. interest rates are changed) and that consumers rely on the altered data to their detriment. This risk could likely be addressed through disclosure that makes clear that the product terms offered by the bank are those that apply at the point of sale and not those disclosed through comparison sites.

70. In contrast, a consumer's transaction data could disclose personal confidences and enable identity theft. Transaction data can disclose an individual's preferences (eg political affiliation as disclosed through donation payments), relationship status (joint account details), health (payments to doctors), location and movement (statement address details, patterns of expenditure) and other personal attributes (as disclosed by expenditure). It can also enable identity theft by allowing malfeasants to convince third parties of a wrongful identity. For example, banks can use last known transactions for identity validation. Of course, these data risks exist today. Customers could lose their paper statements or have their downloaded electronic statement files compromised. Open banking, however, exposes the data sets to a broader range of actors and accelerates the risk.

71. Set out below are high-level risk assessments of the data sets and transfer mechanisms that could support the use cases identified above.

DATA RISK CONSIDERATIONS

Data set and form	Risk of harm to consumer	Discussion	Possible risk mitigant
Product/service attribute data	**Low**	Attribute data does not reveal any details about customers. The commercial information it reveals is already publicly available	None required
Summary of transaction data	**Medium**	Summarised transaction data could raise privacy concerns relating to an individual's financial position, data misuse risks and identity theft potential (from static account information) However, it would not include individual transaction details that could disclose preferences, location and non-financial attributes (like health)	Data security and use standards being applied to data recipients Establishing robust consent and authentication procedures
Complete transaction data	**High**	Complete transaction data would raise the same concerns above but on a heightened scale It could be used to identify preferences, location and non-financial attributes	As above & Not providing complete transaction data where summary transaction data is sufficient

Transfer mechanism	Risk of harm to consumer	Discussion	Possible risk mitigant
Public API (product/service attribute data)	**Low**	Product attribute data would be publicly available and subject to manipulation risk	None required
Download CSV file of transaction data	**High**	Data would be located on consumer's home computer/device and dependent on the data security employed by the consumer	Disclosure to consumer about the risk involved in storing transaction data on their home computer Encryption of data with the consumer given a key by the data transferor
Transmit CSV file of transaction data	**Medium**	Data would be sent securely by data transferor to data recipient Risk would reside in authentication of data recipient and their entitlement to the data (ie the consumer's consent)	Establishing robust consent and authentication procedures
Permissioned API	**Medium**	APIs embed security protocols that help authenticate the recipient and correctly identify the correct data sets If compromised, however, APIs would allow for data theft	As above & Security testing of API framework by data transferor

Risk mitigants

72. The risk mitigants that could be implemented to protect consumer data are the following.

Limit the use of complete transaction data

73. As significant data misuse potential arises from complete transaction data, an appropriate mitigant would be to either:

- Only pursue those consumer use cases that can be enabled with summary transaction data; or
- Limit complete transaction data to those consumer use cases that need it.

As discussed above, personalised comparisons and basic financial management use cases could be achieved using summary transaction data.

Consent and authentication procedures for data recipients

74. The risk of unauthorised use could be reduced (but not eliminated) if there are strong controls in place to ensure that the consumer has freely consented to the data transfer and to authenticate that the data recipient has that consent.

Free consent

75. Consumers need to be able to grant their consent to data transfer freely and clearly. In particular, the requirement for consent to the transfer should guard against behavioural biases and heuristics that may see default settings and oracular disclosure or terms produce consent inappropriately. In addition, consumers should be able to withdraw their consent to the data transfer with immediate effect.

Authentication

76. Only data recipients who have a consumer's consent should be able to access the data of that consumer. This would involve an authentication process by which the consumer's consent can be held by the data recipient and presented to the data transferor who can then confirm the veracity of the consent. The authentication model would vary with the transfer mechanism.

AUTHENTICATION

Transfer mechanism	Authentication process
Download CSV file of transaction data	Consumer is responsible for verifying the identity of the data recipient and whether they consent
Transmit CSV file of transaction data	Consumer selects data recipient from pre-defined list of licensed data recipients within internet banking portal
Permissioned API	The UK open banking project uses OAuth authentication standards Banks could require step-up authentication when delegating 3rd party access to their accounts, and stipulate re-authorisation periodically

Apply data security and use standards to data recipients

77. Ensuring that data is safe in the hands of data recipients could protect both complete and summary transaction data. While data recipients may voluntarily take steps to secure data in order to maintain consumer trust, there would be residual risk that data security was lacking in some firms. Standards would ideally compel data recipients to secure data from unauthorised access and use and require them to only use the data for the purpose for which it was gathered.

78. These standards are already applied by many potential data recipients due to their obligations under the *Privacy Act 1988* (Cth) (**Privacy Act**). However, as discussed below, there are gaps in this framework that could see smaller and offshore data recipients not be obliged to secure data appropriately.

79. Further, the expectations of the privacy regime are not as stringent as the data security standards that are currently applied to banks. Currently, banks are subject to the privacy regime as well as additional supervision with respect to data security under APRA regulation including APRA's *CPG 234 – Management of Security Risk in Information and Information Technology.* This sets an enhanced level of security that bank customers currently benefit from when their data is held by a bank. Further, banks are subject to capital requirements. These mean that they would likely be able to meet a claim for loss arising from a data breach.

80. These points indicate that an appropriate risk mitigant may be the mandatory adherence to prescribed data security standards by non-bank data recipients.

Security testing of API framework by data transferor

81. Protecting APIs from misuse (such as hacking) requires a number of security configurations, including rules on how the API channel is authenticated, how the API itself can be used, from where and how often and ensuring robust token generation algorithms. Tokens for access also need to be individually authorized, and that authorization needs to be verified to prevent misuse, and allow revocation when required. Behavioural analysis techniques can also be used to detect abnormal use of particular tokens, indicating remote compromise.

82. Bank data transferors would be subject to data security requirements under APRA's regulation (see above). Among other things, these requirements see banks needing to test their software and applications for vulnerabilities, undertake penetration and control testing, consider operational resilience, perform incident response drills and test staff. Such requirements would cover the integrity of any API framework that was implemented as part of open banking.

USE CASE ASSESSMENT

Key point

Taking into account the data complexity and risk of the identified use case permutations, simple open banking could require ADIs to make available:

- **Product attribute data via public APIs; and**
- **Summary transaction data via transfer to data recipients or permissioned APIs**

concerning transaction and savings (deposit) accounts.

83. The data required for the identified use cases and the risk involved with making that data available allows an assessment, at a high level, of the various permutations of use case, product, data set and transfer mechanisms. This assessment, set out in the table below, concerns how much data complexity and risk is involved in each use case for each kind of product.

84. Based on this assessment, the simplest use case would involve deposit accounts. This is because these products have the lowest data complexity. They have a low number of attributes and are only offered by ADIs. The simplest way of enabling use cases involving deposit accounts would be to deliver the product attribute data through public APIs and summarised transaction data through transmitted CSV file directly to the data recipient or via permissioned APIs. These data formats and transfer mechanisms would involve the lowest risk.

85. In contrast, complex financial management would require significant amounts of data and pose higher degrees of data risk. This is because consumer's complete transaction data would need to be available through APIs across all their products and financial institutions.

86. If the Independent Review were to follow our suggestions, consumers could take advantage of the following use cases:

    - Generic product comparisons concerning deposit accounts
    - Personalised comparisons concerning deposit accounts
    - Basic financial management, such as expenditure and savings

87. Specific use cases would need to be defined to allow the summary data specifications to be followed by data transferors. We also note that flexibility concerning the transfer mechanism may be prudent given technological innovation.

88. Pursuing a simple form of open banking initially would allow assessment of the degree to which consumers want to engage with open data while not creating a significant implementation challenge.

89. Of course, as set out in the table below, there are degrees between these ends of the spectrum that are possible. If the Independent Review wanted additional use cases to be available, it could consider product attribute data for personal loans and mortgages to allow generic comparisons of those products. These are the next easiest use case.

IMPLEMENTATION CHALLENGE ASSESSMENT

Analysis of data complexity, risk and regulatory requirements that drives implementation challenge assessment

Use case	Product	Implementation challenge assessment	Attribute data complexity	Transaction data needed	Data risk	Transfer mechanism	Transfer risk
Generic comparison	**Deposits**	**Easiest**	Low	**None**	Low	**Public API**	Low
	Personal loans	**Moderate**	Medium				
	Mortgages	**Moderate**	Medium				
	Credit cards	**Harder**	High				
Personalised comparison **&** **Basic financial management**	**Deposits**	**Easiest** for summary data delivered via 'Transmit CSV file' **Moderate** for all other permutation with high risk where consumer download	Low	**Summary**	Medium	**Download CSV file** (for transaction data)	High
	Personal loans	**Moderate**	Medium			**Transmit CSV file** (for transaction data)	Medium
	Mortgages	**Moderate** for summary data delivered via 'Transmit CSV file' **Harder** for all other permutations with high risk where consumer downloads CSV file	Medium	**Complete**	High	**Permissioned API** (for transaction data)	Medium
	Credit cards	**Harder** for all permutations	High				
Complex financial management (real time) **&** **Apply for credit**	**All**	**Harder** for all permutations	High	**Complete**	High	**Permissioned API** (for transaction data)	High

LEGAL REFORMS

Key point

Legal reforms are needed to:

- **Mandate the availability of data**
- **Clarify the liability of data transferors and data recipients**
- **Set up the regulatory framework**

These reforms should be scalable to support economy-wide open data as well as open banking

Introduction

90. Regardless of which permutation of use case, data set and transfer mechanism is pursued, law reform will be required to catalyse and support open banking as well as economy-wide open data. While Australia already has legislation concerning data in the form of the Privacy Act, the Productivity Commission has recommended that its open data reforms be housed in a new act, the *Data Sharing and Release Act*.

91. Laws would perform several functions in the move towards open banking and open data:

    - **Mandate the availability of the data** – A new law would require specified entities to make specified data sets available by a specified date when requested by the consumer. In addition to giving open data legal backing, such a law would help data transferors overcome any legal impediments to making data available

    - **Clarify the liability of data transferors and data recipients** – The law should set out when and how data transferors and data recipients could be liable in law for open banking acts. Critically, the law should clarify that if a data transferor releases or transfers in accordance with a consumer's request, the data transferor then has no liability for any losses of the consumer that arise from the subsequent misuse or loss of the transferred or released data

    - **Set up an appropriate regulatory framework** – The law should provide a framework for the regulatory framework that will underpin open banking and open data more broadly

92. Set out below are our observations on this law reform.

Mandated availability

93. We think that open banking should be catalysed by an enactment that sets out or allows for rule making power to prescribe which entities, to whom and what data needs to be made available. It should also set out the deadline by which this needs to happen.

94. Ideally, the act would set up a framework that allows these prescriptions to be applied beyond the banking sector. This would enable the Government to use the enactment for

economy-wide open data as well as open banking. This would save implementation costs and provide a clear signal to the economy about data availability.

95. If the Independent Review were minded to follow our recommendation, we note that section 1017D of the *Corporations Act 2001* (Cth) (**Corporations Act**) sets out the required content for periodic statements concerning deposit accounts. This section could be used to anchor the mandated availability of summarised transaction data in relation to savings and transaction accounts.

Clarify the liability of data transferor

96. The act should also absolve data transferors from legal liability if they make data available in accordance with the act's mandated availability mechanism. This absolution would have a number of limbs.

Consumer's private right of action for loss

97. There is the risk that consumers suffer losses as a result of the data being transferred from data transferor to data recipient. The recipient may not protect the data as well as it should or it may misuse the data itself. In circumstances where the data recipient is insolvent or not well capitalised, consumers may seek redress for their losses from the data transferor.

98. To minimise the risk of mandated availability to data transferors, the act should be clear that provided data transferors follow the appropriate consent and authentication procedures, and transmit the data to the data recipient in accordance with any standards, then they will be absolved from legal liability for the consequential use, misuse or loss of the transferred data.[18]

Data recipient loss

99. Data transferors need to be absolved from the reliance by data recipients on the data. For example some aspects of a bank's data on a person will be misleading in isolation. An account statement may show repayments of a loan being made but not disclose that the account is under a hardship application. Data transferors should just be under an obligation to disclose the requested data as it appears on their systems. The provision of such information should not imply that there is no other data that would also be relevant.

100. This reform will be particularly important for summarised transaction data where the data transferor is analysing and transforming (ie extracting and aggregating) the data for the data recipient's use.

Safe harbour from contractual breach

101. Data transferors should be granted a safe harbour from breach of contract actions in situations where the disclosure of the data (and the immediate preparatory acts connected

[18] The Productivity Commission recognised the utility of such a protection in its report: Ibid, 338.

with the disclosure) may be considered to breach a contract to which the data transferor is party. For example, some IT vendor agreements governing software used to store and process data limit the ability of licensees to use the outputs for 'internal business purposes'. In other instances, the data generated can only be used in conjunction with proprietary software. Similarly, there are restrictions on data use under the Payment Card Industry Data Security Standards that may come into conflict with mandated data availability. Further, we note that there is a risk that the data recipient may be found to be an indirect user of software licensed by the bank with consequential cost implications, depending on the licensing model for that software.[19] These points should be addressed in the law reform.

Intellectual property exception

102. However, there should be a carve-out from the obligation to make data available if it would contravene the IP rights of a party other than the data transferor or the data recipient. This is necessary to address situations where an Australian regulatory framework providing safe harbour from contractual breach is not applicable, for example in relation to third parties not bound by Australian law.

Amendments to Australian Privacy Principles

103. The new act should also clarify the data transferor's obligations under the Privacy Act.

AMENDMENTS TO PRIVACY REGIME

Australian Privacy Principle	Suggested amendment
Australian Privacy Principle 6 Use or disclosure of personal information	Make clear that disclosure through open banking is consistent with this principle
Australian Privacy Principle 7 Direct marketing *Individual may request not to receive direct marketing communications etc.*	Make clear that data transferor has no obligation to disclose or investigate whether data recipient intends to engage in direct marketing to consumer
Australian Privacy Principle 8 Cross border disclosure of personal information	Make clear that APP 8 has no application in relation to cross border transfer in accordance with open banking
Australian Privacy Principle 9 Adoption, use or disclosure of government related identifiers *Use or disclosure of government related identifiers*	Make clear that APP9 has no application to the extent that data transferors are obliged to disclose Government-related identifiers in accordance with open banking
Australian Privacy Principle 10 Quality of personal information	Make clear that APP10.2 has no application in relation to data transferred in accordance with open banking as the data transferor will have no visibility of the purpose of disclosure. The data transferor's sole obligation should be to provide

[19] See *SAP UK Ltd v Diageo Great Britain Ltd* [2017] EWHC 189 (TCC) (16 February 2017)

Australian Privacy Principle	Suggested amendment
	the requested data as it is currently held by the data transferor.
Australian Privacy Principle 11 Security of personal information	Make clear that data transferors should have no responsibility for the security of the information after it leaves the data transferor's firewall. At this point liability for security passes to the data recipient
Australian Privacy Principle 12 Access to personal information	This right will work in tandem with the open banking mandate on the assumption that data transferred under open banking will only ever be a subset of personal information
Australian Privacy Principle 13 Correction of personal information *Notification of correction to third parties*	This obligation should not apply if the data recipient is no longer a participant of the open banking regime e.g. where it no longer complies with the data security standards (discussed below under 'Regulatory Framework')

Set up an appropriate regulatory framework

104. Legal reform is also required to ensure that the regulatory framework is robust.

105. This would include both adapting the existing regulatory framework concerning privacy and putting in place a new framework that supports open banking and economy-wide open data. Our views on the appropriate regulatory framework are set out below.

Remove Privacy Act carve outs

106. Amendments to the Privacy Act would include the closing of certain exceptions that could see data transferred to data recipients with no obligation to protect the data of the consumer or to use it for the purpose for which the consumer consented to its disclosure.

107. Two critical exceptions are:

- Entities that do not have an Australian link (section 5B(2) and (3) Privacy Act)
- Entities that turn over $3 million or less annually (section 6D Privacy Act)

108. Both of these exceptions should be removed for entities in respect of data received under open banking and, indeed, open data when it is implemented.

Consent for use requirements

109. The Privacy Act already has requirements that a consumer's consent is obtained for the use for which the data is to be used. This requirement will be important in open banking environment where consumers will likely be consenting to, or requesting, the transfer of their data for specific purposes. It may be appropriate to ensure that the consent requirements are well calibrated for open banking (and open data).

110. Further, we would suggest that the issue of consent for joint account holders needs to be addressed. The safest approach would be for the consent of all signatories to the account to be obtained.

A new data-related act

111. In considering whether this law reform resides in an existing or new enactment, we refer to the principle articulated above that *economy-wide open data should be the end-state of open banking*. This means that whatever enactment is used to catalyse and underpin open banking should be scalable to doing the same for economy-wide open data.

112. This suggests that the finance-specific legislation (eg *Banking Act 1959* (Cth), Corporations Act, *Australian Securities and Investments Commission Act 2001* (Cth) and *Australian Prudential Regulation Authority Act 1998* (Cth)) would not be appropriate.

113. Further, consistent with the observations of the Productivity Commission, we question whether the Privacy Act is the appropriate vehicle for an era predicated upon the importance of data.[20] As electronic data and its use become more embedded in our economy, we can see the importance of a legislative framework that can articulate community expectations at the scale that will be required. A new act may future proof Australia's laws concerning electronic data. Related to this is the importance of facilitating economy-wide open data in the near term. An act that can support both open banking and economy-wide open data makes sense.

114. As such, it may be appropriate to consider a new act that provides for both open banking and economy-wide open data. The Government may like to consider enacting a new Data Act that would be modelled on the *Data Sharing and Release Act* with scope to provide for data protection as appropriate. This new Data Act could include open banking as a specific iteration of economy-wide open data. This could occur through a rule making power or similar designation mechanism.

[20] Ibid, 310.

REGULATORY MODEL

Key point

The regulatory model should set standards for both data availability and data security. It should also provide for monitoring of initial and ongoing compliance with those standards.

The regulatory framework for data transferors should include data format standards coupled with the compliance mechanism that is intended to be used for economy-wide open data (eg consumer right of action with Government oversight).

The regulatory framework for data recipients should include data security standards that are enforced through a mix of informing consumers, a private right of action for breach of the standards, Government oversight and licensing.

Introduction

115. Related to the legal reforms is the regulatory model that accompanies open banking, and open data more broadly. This regulatory model should undertake three broad functions in addition to providing oversight of open banking/data. The functions apply to both data transferors and data recipients. Within each of these functions is the question of who sets standards and enforces compliance.

REGULATORY MODEL FUNCTIONS

Function	Detail	
	Concerning data transferors	Concerning data recipients
Overall oversight	Government agency responsibility for the implementation of open banking/data	
Standard setting	Set the technical standards concerning the type and format of the data that needs to be made available (**data standards**)	Set the standards concerning data security and use (**security standards**)
Initial compliance	Make data available by the implementation date	Administer and enforce any initial accreditation, registration or licensing obligations to become an authorised data recipient
Ongoing compliance	Monitor compliance with consumer requests for data transfers and data transfer consent standards	Monitor compliance with data security standards and data transfer consent standards

Oversight of open banking

116. The initial regulatory issue is the Government agency that should be tasked with overseeing open banking. This role would involve being the relevant agency under any enactment, being vested with any regulatory functions and advising on and setting relevant policy.

117. We have do not have opinion on which entity should be selected. Our preference would be an existing entity that is capable of having a remit beyond open banking to include economy-wide open data. The remit should incorporate and combine the policy objectives of privacy and innovation. This would allow the agency to foster an economy where data is viewed and used as a valuable resource as well as an attribute that concerns individual dignity.

Data transferors

Standard setting

118. The primary regulatory function concerning data transferors is the setting of the data format standards. The need for these standards would vary with data type and data transfer method.

NEED FOR DATA STANDARDS

Data and transfer mechanism	Required standards	Complexity
Product attribute data via APIs	API standards – standards concerning the APIs used Data format – standards concerning how the data is organised and presented	Complex
Download/transmit CSV file of summary transaction data	Data format – standards concerning the required fields of summary data to support each use case	Less complex
Download/transmit CSV file of complete transaction data	None required	Less complex
Permissioned API for summary transaction data	API standards – standards concerning the APIs used Data format – standards concerning the required fields of summary data to support each use case	Complex
Permissioned API for complete transaction data	API standards – standards concerning the APIs used	Complex

119. Development of these standards could be undertaken by a body with sufficient technical expertise and the ability to take into account the views of both data transferors and data recipients as well as the interests of consumers. This could be a Government agency, existing standard setting body, industry body or new special purpose entity.

120. Funding the body may be done by data recipients contributing to its cost or, as discussed below, data transferors recovering the cost through a charging model for data transfers.

121. Critically it is not necessary that the body that develops the standards perform the other regulatory functions concerning data transferors. Thus, a model might be that the standard setting body is tasked with developing the standards that a Government agency is then responsible for seeing implemented by industry.

Compliance (initial and ongoing)

122. Overseeing initial compliance by data transferors could rest with the Government agency that has overall oversight of open banking. In contrast, ongoing compliance with the obligation to make data available could be overseen through a number of different regulatory methods.

POSSIBLE REGULATORY METHODS FOR ONGOING COMPLIANCE

Method	Detail
Private right of action	Consumers have a right to transfer their data that they can enforce against bank (eg like the 'comprehensive right' proposed by Productivity Commission)
Self-regulation	An industry body oversees compliance with open banking mandate
Government	A Government agency enforces compliance with open banking mandate

123. The preferable method would be the one that is most aligned with the model that will be implemented for economy-wide open data. As such, it may be preferable to grant individuals a right to obtain relevant data from data transferors with compliance monitoring undertaken by the Government agency that has overall oversight of open banking.

Data recipients

124. The regulatory framework that applies to data recipients should keep consumer bank data safe and, through that, trust in open banking strong.

Standard setting

125. Standards concerning data security already exist. To the extent needed, these could be formally incorporated into the open banking regulatory framework. Some of these standards are set out below:

- ISO 27001:2013 – Information Security Management Systems (International Standards Organisation)
- ISO 27002: 2013 - Code of Practice for Information Security Controls (International Standards Organisation)
- NIST SP800 – Computer Security (National Institute of Standards and Technology)
- NIST SP800-53 R4 – Risk Management Framework, including Appendix J – Privacy Controls (National Institute of Standards and Technology)
- PCI DSS v3- Protection of Payment Card Information (Payment Card Industry)
- FIPS 140-2, 180-4, 186-4, 197, 198-1 – Federal Information Processing Standards (National Institute of Standards and Technology)
- ISM 2016 - Information Security Manual (Australian Signals Directorate)
- Essential 8 – Strategies to Mitigate Cyber Security Incidents (Australian Signals Directorate)

126. In addition to the data security standards, collateral protections may also be relevant, including:

- Financial resource requirements for data recipients to ensure that they can meet claims by consumers for data misuse; and
- Complaints handling paths for consumers, including an internal mechanism and membership of an external dispute resolution scheme.

Compliance (initial and ongoing)

127. The more challenging component of regulating data recipients concerns how to enforce and monitor compliance with the data security standards. As set out below, there are a number of possible regulatory methods that could be employed.

RANGE OF REGULATORY METHODS FOR DATA SECURITY STANDARD COMPLIANCE (INITIAL AND ONGOING)

Method	Detail	'Regulator'	Potential effectiveness in protecting data	Barrier to becoming a 'data recipient'
Education	Government runs an education campaign concerning data sharing to help consumers understand risks (and benefits) of data sharing	Consumer	Low – alone, this relies on consumers disciplining data recipients	None
Information	Consumer is provided with mandatory disclosure by data recipient about data sharing risks and the data security methods of data recipient (including, potentially, their historical record in keeping data safe)	Consumer (with Government enforcing mandatory disclosure)	Low – alone, this relies on consumers disciplining data recipients	Minimal – just need to be able to provide information
Contractual (Consumer and data recipient)	Data recipients are obligated to enter into contracts with consumers concerning how they will protect the consumer's data	Consumer (and courts or external dispute resolution service)	Low – alone, this relies on consumers disciplining data recipients	Moderate –must keep data secure to contracted standards
Private right of action	Consumers have a private right of action against data recipients by act (rather than contract) if data recipient does not keep data secure	Consumer (and courts or external dispute resolution service)	Moderate – potential for class-action may impose discipline on data recipients	Moderate – must to keep data secure to avoid court action
Contractual (Data transferor and data recipient)	If data transferors select data recipients (eg for the *Transmit CSV file of transaction data* transfer method), then data transferor and data recipient would enter into contract obliging data recipient to keep transferred data secure	Data transferor (and courts)	Moderate – however, relies on data transferors policing data recipients – this has agency-mismatch and cost-allocation problems and requires multiple bi-lateral negotiations	Moderate – must keep data secure to contracted standards
Accreditation (voluntary)	Data recipients have the option of being accredited against data security standards by recognised body (Government or private). Data recipients need to disclose their accreditation (or lack thereof) to consumers (ie use in conjunction with 'Information')	Accrediting body and consumer	Moderate – provides for homogenised standards and independent vetting	Moderate – accreditation status may act as quality indicator in market
Negative licensing	No license is required for data recipients to accept consumer data but if they fail to keep it safe, a Government agency is entitled to bring an action against them (similar to 'Private right of action')	Government agency	Moderate – data recipients would have strong incentive to comply	Moderate – must keep data secure to avoid court action
Registration	Data recipients are required to register with Government agency but do not need to meet any minimum standards. Could be used in conjunction with 'Negative licensing'	Government agency	Higher – this would be most effective when coupled with negative licensing	Moderate – just need to register with Government
Licensing	Data recipients must have a license from Government agency that involves assessment against qualitative data security standards and, potentially, minimum financial resources requirements as well as membership of an external dispute resolution body	Government agency	Higher – this would require data recipients to obtain licence	Higher– depends on content of licensing requirements

128. The range of regulatory methods that can be used to persuade adherence by data recipients to a set of data security standards is broad. Identifying the optimal method or methods involves a calibration of the effectiveness of the regulatory method in protecting consumer's data against the potential barrier to entry that it poses to data recipients participating in the market.

129. Under current Australian law, the privacy regime is effectively one of information, private right of action and negative licensing. Consumers are told about data collection and use and both the Government and individuals can bring actions if data holders do not comply with the privacy principles. We have suggested gaps in this regime that should be filled.

130. We think it would be appropriate to explore whether additional regulatory methods should supplement the privacy regime for open banking and open data. Under the privacy regime, entities need to take 'reasonable steps' to protect data. Because of the harm that could arise from compromised transaction data, there should be minimum data security standards that apply to data recipients receiving this type of data.

131. The regulatory model to achieve this in respect of open banking could be the following. These requirements below should apply to all data recipients regardless of size or geographical location.

RECOMMENDED REGULATORY MODEL FOR DATA RECIPIENTS

Method	Detail
Information	All data recipients need to provide consumers with clear and prominent disclosure about: • The intended use of the data; and • The steps that will be taken to protect it
Private right of action	Consumers should have the right to bring an action if data recipients: • Use the data other than for the consumer use case or as disclosed • Do not take reasonable steps to protect the data The costs of bringing the right of action could be reduced if consumers were entitled to bring an action to a non-court dispute resolution scheme (eg financial sector recipients will likely be subject to the jurisdiction of the new Australian Financial Complaints Authority) or to the relevant Government agency
Licensing	Data recipients wishing to receive consumer bank data should be required to obtain a license from a Government agency. This would ensure that recipients comply with agreed data standards and that data transferors and consumers can verify the status of a data recipient. This would help data transferors know that it is safe to include an entity on their list of possible data recipients when offering transfer options through internet banking.

132. These combined regulatory methods would likely have the effect of causing compliance by data recipients with agreed data security standards. We think that this regime would be appropriate to support economy-wide open data. Obviously, Government may want to consider the calibration of the requirements based on the sensitivity of the data.

COMPETITION

Key point

Open banking should support competitive neutrality by allowing data transferors to charge data recipients for the data and by economy-wide open data being implemented soon after open banking

Introduction

133. One of the principles that we proposed for open banking is that it not introduce competitive distortions. This does not mean that open banking should not drive competition through more empowered consumers. Indeed, we believe that consumers should be enabled to be more discriminating and understanding demand-side actors. Rather, it means that open banking should not advantage one set of providers over another and allow them to win consumers through Government policy instead of better products and services.

134. The open banking regime should not enable the transfer of a valuable resource (data) from one set of competitors to another without a reciprocal value exchange. We believe there are several policy settings that could be adopted to ensure open banking does not distort the competitive field while still allowing consumers the ability to use their data.

Charging for the transfer of data

135. The issue of charging for data transfers within open banking (or open data more broadly) involves a triumvirate of interests. Consumers have an interest in transferring data concerning them so that they can access new services. Data recipients have an interest in receiving that data so that they can provide those services to the consumer for a profit. Data transferors have an interest in helping their customers but not in aiding the business models of their actual or potential competitors.

136. Reconciling these interests in a way that adheres to the principles we outlined above concerning consumer interests and competitive neutrality is difficult. The Productivity Commission recognised that data transferors could charge consumers for data transfers, in part to dissuade 'spurious' transfer requests.[21] Excessive charging, however, may chill consumers' interests in transferring their data. Further, consumers could view the data as theirs. Completely free data, though, would not recognise the efforts of data transferors in collecting, storing and protecting the data and the commercial interest that the data recipient has in receiving the data.

[21] Ibid, 221.

137. One way of reconciling these interests is to agree a charging model for data transfers under the auspices of a Government agency and with appropriate representation of the interests detailed above. Such a model could set a price for data transfers that recognises:

- The consumer's interest in the data and the potential utility that they may derive from services based on that data;
- The efforts and cost of the data transferor in maintaining and making available the data; and
- The potential commercial benefit that may accrue to the data recipient.

138. It may be that this charging model sets a schedule of prices that would be paid by data recipients for transfers based on data type, transfer mechanism and transfer frequency.

Economy-wide open data as end-state

139. Economy-wide open data would see all data custodians providing equal (ie reciprocal) access to the data that they hold. This would mean that consumers would be able to transfer data from one sector of the economy to another. Open banking should be implemented as transition point as Australia moves towards economy-wide open data. This will reduce the risk of data flowing out of one sector due to its regulatory status only.

Clear limitations on use

140. If open banking is implemented on the basis of enabling use cases, any transferred data could be limited to supporting those use cases. While this may restrict the consumer's right to use their data as they see fit, this may be appropriate while open banking is developing. Once data becomes broadly available through the economy, we would agree that no limitations should be applied to data's use after transfer to the data recipient (subject to the consumer's consent to the use).

Standardisation of data

141. As we noted above, the standardisation of data fields could ossify products if the law states that data transferors cannot offer products if they do not also offer standardised product attribute data on the product. There needs to be a mechanism to allow for innovation in products while still allowing for comparisons by consumers.