Australian Government

OPEN BANKING

customers
choice
convenience
confidence

December 2017

REVIEW INTO OPEN BANKING:
giving customers choice, convenience and confidence

DECEMBER 2017

ISBN 978-1-925504-72-9

Manager
Communications
The Treasury
Langton Crescent Parkes ACT 2600
Email: **medialiaison@treasury.gov.au**

Contents

Foreword

Open Banking gives customers a right to direct that the information they already share with their bank be safely shared with others they trust. It is designed to give customers more *control* over their information, leading to more *choice* in their banking and more *convenience* in managing their money, and resulting in more *confidence* in the use and value of an asset mostly undiscovered by customers – their data.

Open Banking is part of the Consumer Data Right in Australia, a more general right being created for consumers to control their data, including who can have it and who can use it. Banking is the first sector of the Australian economy to which this right is to be applied and Open Banking is the way that this is to happen. More sectors of the economy are to follow and Open Banking needs to work together with them to form a single, broader framework.

Starting with banking makes sense because of the firm foundation provided by the duties that a bank owes its customer. A bank has a duty to keep a customer's money safe and to pay it to others at the customer's direction. Similarly, a bank has a duty to keep its customer's information confidential. An obligation for a bank to provide the customer's information to others at the customer's direction makes sense – both money and information are valuable and the bank would not have either without the customer. In this way, the long-established banker-customer relationship can help guide Open Banking's construction and once the framework is built, it can be extended to other sectors.

Of course, there is much more to Open Banking. This Report sets out detailed findings and recommendations to many complex and challenging issues. However, four simple principles have emerged:

- 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.

These principles of who Open Banking should be for, why it should be done, what it should do and how it should be achieved, have guided this Review, in its decisions and deliberations, its consultations and conversations and in preparing this Report and its recommendations.

Although this Report focusses on how Open Banking should be done, it is worth sparing a moment to consider what Open Banking could mean in the future. Improving the control, choice, convenience and confidence of customers should, in the longer term, create a customer-centric data sector which generates growth and employment and, importantly, value to customers by increasing the safe and efficient access to data. The new services, new products and new skills inspired by Open Banking which benefit customers are likely to be in demand not only in Australia but also overseas. Indeed, the pace of similar developments elsewhere in our region shows that this potential is already understood beyond our shores.

Another benefit is that the greater availability of data should allow Australian data science knowledge, expertise and experience to grow. Data is important for critical scientific fields for our future, including artificial intelligence and machine learning. A further advantage is that the increased use of data should make it easier to work out the value of data. This would improve the fairness, efficiency and transparency of data sharing arrangements. Customers who choose to share their data are more likely to share *in* its value if they know what that value is. Also, knowledge that their data is valuable should assist customers in appreciating the responsibility they have for their choices to share their data with others.

Of course, achieving these longer term benefits would require care, as well as encouragement. Systems are likely to be needed to monitor, assess and manage additional risks arising through the broader and deeper use of data. Fortunately, the principles used with money, communications and energy systems should show what could be needed for the sustainability of a stable, broader data ecosystem. Establishing this will be important further work.

I express my warm thanks to everyone who has contributed to this Review, including the many who have taken the time to meet with me, speak to me and work with me, on the diverse range of issues and concerns which have been considered. I am enormously grateful for the vast amount of knowledge, expertise and experience which has been contributed from the banking, FinTech, consumer, technology and regulatory communities. My deepest thanks I save for the professional, patient and tireless officers of my secretariat, without whom I could never have completed this challenging task.

Scott Farrell

Executive Summary

What has the Review been asked to do?

In the 2017-18 Budget the Treasurer, the Hon. Scott Morrison MP, announced that the Government would introduce Open Banking in Australia. In July 2017 the Treasurer commissioned this Review into Open Banking with a brief to report to him by the end of 2017. The key task for the Review is to recommend the best approach to implementing Open Banking.

Specifically, the Review has been asked to recommend 'a regulatory framework under which an open banking regime would operate and the necessary instruments (such as legislation) required to support and enforce a regime', and to do so in a way that has regard to the Productivity Commission's Data Availability and Use Inquiry (the PC Data Report), international best practice, competition, fairness, innovation, efficiency, regulatory compliance costs and consumer protection.

Since the Review was given its original Terms of Reference, the Government announced that it will introduce a Consumer Data Right.[1] The Consumer Data Right will provide consumers with rights to direct that a business transfer data on the consumer to a third party, in a usable machine readable form. The announcement stated that implementation of the Consumer Data Right will be prioritised in relation to banking, energy and telecommunications data. Open Banking is the implementation of the Right in relation to banking data and that the design of the broader Consumer Data Right will be informed by the findings of the Open Banking Review.

Overview of findings and recommendations

The Government's decision to implement Open Banking as the first application of the Consumer Data Right aims to facilitate an economy-wide consumer-directed data transfer system. Therefore, when designing Open Banking, the Review has kept interoperability between sectors in mind. Interoperability means that what has been designed for the banking sector will also be able to work in other, different, sectors of the economy (for instance, energy and telecommunications).

The process of designing this system has been highly consultative. In the five months since it was commissioned, the Review has had over 100 meetings with banks, firms, industry bodies, consumer groups, regulators, and data specialists. It has considered formal submissions from 41 interested parties. It has also consulted with Open Banking participants in other jurisdictions to understand their experience. Further information on the consultation undertaken by the Review is contained in Chapter 1, and formal submissions are listed in Appendix B.

1. Available at: https://ministers.pmc.gov.au/taylor/2017/australians-own-their-own-banking-energy-phone-and-internet-data

The Review has collected its recommendations in the following Chapters:

- Chapter 1 sets out the context for the Review, including the current state of data sharing, views on Open Banking from interested parties, the goals being sought by the reforms and the approach adopted by the Review.
- Chapter 2 maps out the regulatory framework that should apply to both the Consumer Data Right and Open Banking, including the responsibilities of regulators and those within the system.
- Chapter 3 makes recommendations on the scope of Open Banking, explaining which data should be affected and identifying the eligible participants.
- Chapter 4 deals with the safeguards required to maintain confidence in the system, including expanding certain confidentiality principles and remedies beyond their current ambit, and clarifying liability.
- Chapter 5 canvasses technical aspects of the data transfer mechanism, and gives guidance to enable Rules and Standards to be established.
- Chapter 6 deals with implementation issues and other matters that may need to be considered in future, or as part of the next phase of the Consumer Data Right.

A number of issues of detail are dealt with in the appendices.

Chapter 1 – Context for the Review

A number of recent Government Reviews and Inquiries have recommended expanding consumers' access to data. Open Banking is an early implementation of reforms that will grant customers this access. Banks currently capture the value of customer banking data. Open Banking aims to share this value with customers by giving them greater access to, and control over, their banking data. By doing so, Open Banking has the potential to transform the banking system. The Review has designed an Open Banking system that is customer-focused, efficient and fair. Ideally, the system will inspire confidence, promote competition and encourage innovation. In mandating Open Banking, the Government should be careful to leave other avenues open in order to promote competition and test the system design.

Chapter 2 – Regulatory framework

Open Banking should be legislated through amendments to the *Competition and Consumer Act (2010)*. It should be regulated by the ACCC (competition and consumer issues and standards setting) supported by the OAIC (privacy protection), with ASIC, APRA and the RBA providing advice as required.

Open Banking should have specific Rules that consider the characteristics of the banking sector as well as interoperability across the economy-wide data transfer system. In addition to these Rules, Open Banking should require technical Standards that specify how participants will connect and how they will meet the Rules. These Standards should be determined by a Data Standards Body, in conjunction with the regulators. The Rules should be general enough to facilitate innovation and the Standards able to change to support this innovation.

Open Banking's success depends on there being trust in the participants that operate in the system. Accreditation for participants should create this trust by requiring data holders and data recipients to comply with a set of standards (including security standards) determined by the regulators of the system. This accreditation system should be tiered, based on the risk of the data set and the participant, and a list of accredited participants should be published in an address book. The idea of 'passporting' accredited participants from systems in other jurisdictions may be considered, once Open Banking systems become more established locally and overseas.

Customers and accredited participants should have access to a robust dispute resolution method.

Chapter 3 – Scope

Open Banking requires data holders to share customer data with a data recipient at that customer's direction. The data and participant scope is critical in determining the success of the system.

The Review considers that the data required to be shared is customer-provided data, transaction data that is stored in a digital form for specific types of accounts held in Australia and product data. Data should be transferred free of charge. However, the following data should not be in scope: data supporting an identity verification check; any data that would materially increase the risk of customer identity theft; aggregated data; and transformed data. The role performed by transfers of data supporting an identity verification assessment can be better addressed by transfers of confirmation that an identity verification assessment has been performed.

Open Banking should require all Authorised Deposit-taking Institutions (ADIs) (other than branches of foreign banks) to share customer data, phased in over time. Non-ADI participants in Open Banking should also be required to share customer data and any other customer data they have acquired in the system. Data sharing should be applicable for all customers with a relevant account in Australia.

Chapter 4 – Safeguards

Open Banking should have safeguards to protect the privacy, security and accountability of all participants.

Open Banking should require informed, explicit customer consent. Data should only be shared when the customer has given an explicit direction to the data holder to do so. This direction to share data should be consistent with the existing authorisations on that account (for example, for joint accounts, the ability to authorise data sharing should reflect the ability to transfer money from that account). Customers should be notified of the data they are sharing and be able to revoke access easily. Customers should find it easy to understand the implications of their actions in Open Banking. This means data holders' notification of a customers' requests and data recipients' consent to use cases should be limited to a single screen respectively.

The *Privacy Act 1988* (Privacy Act) should continue to protect customer data under Open Banking. All businesses (including small businesses) which are accredited to participate in Open Banking should also be required to comply with the Privacy Act. The applications of the protections of the Australian Privacy Principles should be modified in Open Banking to strengthen customer confidence.

Small business customers should have similar access to alternative dispute resolution services for confidentiality disputes to that of consumers under the Privacy Act. And, in order to gain and maintain accreditation, entities should comply with security standards set by the Data Standards Body.

A principles-based, comprehensive liability framework should be established, underpinned by the premise that data-related liability should be allocated to participants for their own conduct, but not the conduct of other participants in the system.

Chapter 5 – Data transfer mechanism

Customer data should be transferred via APIs. These APIs should be built in accordance with the Standards. The Australian Data Standard Setting Body, chaired by an independent data specialist, should design these Standards (using the UK's technical specification as a starting point). The Standards should not mandate specific technology and should not intend to restrict innovation for data transfer. The Standards should enable basic functionality for Open Banking, but they should also be useful for other sectors.

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

The starting point for developing the Standards for authorising the transfer of banking data should be a redirect-based model, although a low-friction decoupled approach should also be considered. Banks should not be permitted to create additional barriers for customers using consent (for instance, by restricting use cases) although multifactor authorisation should be considered reasonable as a security measure. Customers should be able to grant persistent authorisation and manage this authorisation transparently. All authorisations should have an expiry date. The Standards should also allow data access for intermediaries such as middleware providers.

The Standards should determine the frequency of API calls by third parties (including whether push functionality should be available).

Customers who do not use internet banking should still be able to share their data with third parties through service channels which are already offered by their bank.

Customers should be able to see their Open Banking interactions. This means participants should be required to maintain a record of data transfers. Participants should also be required to maintain information on API performance to be provided to the regulator if requested.

Chapter 6 – Implementation

A period of approximately 12 months should be allowed from a final Government decision on Open Banking for implementation (the Commencement Date). The ACCC should be empowered to adjust the Commencement Date if necessary.

The steps to implementation include amending existing laws and regulations, determining roles of regulators and agencies, settling and promulgating Rules, establishing an accreditation framework and setting criteria, establishing a Data Standards Body and setting Standards and IT building and testing by Open Banking participants.

The four major Australian banks should be required to comply with a direction to share data under Open Banking from the Commencement Date. All other ADIs should be required to participate 12 months later, unless this is deferred by the Regulator.

Open Banking should begin by requiring transaction and product data to be available for transfer at the direction of the customer. The timing for implementation of customer-provided data should be determined by the Regulator once consideration of proposed AML law reforms has been finalised.

Consumer education is important to the success of Open Banking. Customers will only use Open Banking if they understand and trust it. All Open Banking participants should play a role in this education, including banks and FinTech firms, as well as the Government, industry bodies and consumer advocacy groups. The ACCC should coordinate and implement a timely consumer education programme.

Open Banking should be formally evaluated 12 months after the Commencement Date. Other post-implementation issues to be considered include:

- the potential for future write access
- the emerging comprehensive digital identity
- a new data ecosystem to advance the digital economy
- greater transparency in the value of data, and
- interoperability with different jurisdictions.

Summary of recommendations

Chapter 1: Context for the review

Recommendation 1.1 – allowing for competing approaches

Open Banking should not be mandated as the only way that banking data may be shared.
Allowing competing approaches will provide an important test of the design quality of Open Banking and the Consumer Data Right.

Chapter 2: Open Banking regulatory framework

Recommendation 2.1 – a layered regulatory approach

Open Banking should be implemented primarily through amendments to the *Competition and Consumer Act 2010* that set out the overarching objectives of the Consumer Data Right. The amendments should enable the designation of a sector by Ministerial direction and create the power to set out regulations and operational Rules for sectors. This structure will embed a customer and competition focus in Open Banking, while allowing the Consumer Data Right to be scalable across sectors.

Recommendation 2.2 – the regulator model

Open Banking should be supported by a multiple regulator model, led by the ACCC, which should be primarily responsible for competition and consumer issues and standards-setting. The OAIC should remain primarily responsible for privacy protection. ASIC, APRA, the RBA, and other sector-focussed regulators as applicable, should be consulted where necessary.

Recommendation 2.3 – the banking Consumer Data Right

Banking should be designated as a sector to which the Consumer Data Right applies.

Recommendation 2.4 – Rules written by the ACCC

The ACCC, in consultation with the OAIC, and other relevant regulators, should be responsible for determining Rules for Open Banking and the Consumer Data Right. The Rules should be written with regard to consistency between sectors.

Recommendation 2.5 – the Standards

The Standards should include transfer, data, and security standards. Allowing supplemental, non-binding, standards to develop (provided they do not interfere with interoperability) will encourage competitive standards-setting and innovation.

Recommendation 2.6 – a Data Standards Body

A Data Standards Body should be established to work with the Open Banking regulators to develop Standards. This body should incorporate expertise in the standards-setting process and data-sharing, as well as participant and customer experience.

Recommendation 2.7 – accreditation

Only accredited parties should be able to receive Open Banking data. The ACCC should determine the criteria for, and method of, accreditation.

Recommendation 2.8 – the accreditation criteria

Accreditation criteria should not create an unnecessary barrier to entry by imposing prohibitive costs or otherwise discouraging parties from participating in Open Banking. Using a tiered risk-based accreditation model and having regard to existing licensing regimes should minimise costs for many participants. Accreditation decisions should be reviewable by the Administrative Appeals Tribunal.

Recommendation 2.9 – responsibility for the address book

The ACCC should have responsibility for ensuring there is a public address book showing who is accredited.

Recommendation 2.10 – customer complaints and remedies

Open Banking should have internal and external dispute resolution processes to resolve customer complaints. Amendments to the *Competition and Consumer Act 2010* should create powers to address complaints (to the extent these do not already exist) and give customers standing to seek remedy for breaches of their rights. There should be a single consumer data contact point - there should be 'no wrong door' for customers. The OAIC should retain enforcement powers in relation to privacy and could also be given enforcement powers of confidentiality for businesses.

Recommendation 2.11 – remedies for accredited parties

The Rules should create a right for accredited parties to seek remedy for breaches of the Consumer Data Right. There should also be breach-reporting obligations to the ACCC.

Chapter 3: The scope of Open Banking

Recommendation 3.1 – customer-provided data

At a customer's direction, data holders should be obliged to share all information that has been provided to them by the customer (or a former customer). However:

- The obligation should only apply where the data holder keeps that information in a digital form.
- The obligation should not apply to information supporting an identity verification assessment. Data holders should only be obliged to share that information with the customer directly, not a data recipient.

Recommendation 3.2 – transaction data

At a customer's (or former customer's) direction, data holders should be obliged to share all transaction data in a form that facilitates its transfer and use. The obligation should apply for the period that data holders are otherwise required to retain records under existing regulations. Table 3.1 describes the list of accounts and other products to which this obligation should apply.

Table 3.1: Proposed list of banking products

Deposit products	Lending products
Savings accounts	Mortgages
Call accounts	Business finance
Term deposits	Personal loans
Current accounts	Lines of credit (personal)
Cheque accounts	Lines of credit (business)
Debit card accounts	Overdrafts (personal)
Transactions accounts	Overdrafts (business)
Personal basic account	Consumer leases
GST and tax accounts	Credit and charge cards (personal)
Cash management accounts	Credit and charge cards (business)
Farm management deposits	Asset finance (and leases)
Pensioner deeming accounts	
Mortgage offset accounts	
Trust accounts	
Retirement savings accounts	
Foreign currency accounts	

Recommendation 3.3 – value-added customer data

Subject to Recommendation 3.4, data that results from material enhancement by the application of insights, analysis or transformation by the data holder should not be included in the scope of Open Banking.

Recommendation 3.4 – identity verification assessments

If directed by the customer to do so, data holders should be obliged to share the outcome of an identity verification assessment performed on the customer, provided the anti-money laundering laws are amended to allow data recipients to rely on that outcome.

Recommendation 3.5 – aggregated data

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

Recommendation 3.6 – product data

Where banks are under existing obligations to publicly disclose information on their products and services — such as information on their price, fees and other charges — that information should made publicly available under Open Banking.

Recommendation 3.7 – application to accounts

The obligation to share data at a customer's direction should apply for all customers holding a relevant account in Australia.

Recommendation 3.8 – application to ADIs

The obligation to share data at a customer's direction should apply to all Authorised Deposit-taking Institutions (ADIs), other than foreign bank branches. The obligation should be phased in, beginning with the largest ADIs.

Recommendation 3.9 – reciprocal obligations in Open Banking

Entities participating in Open Banking as data recipients should be obliged to comply with a customer's direction to share any data provided to them under Open Banking, plus any data held by them that is transaction data or that is the equivalent of transaction data.

Recommendation 3.10 – eligibility to receive data

Authorised Deposit-taking Institutions (ADIs) should be automatically accredited to receive data under Open Banking. A graduated, risk-based accreditation standard should be used for non-ADIs.

Recommendation 3.11 – no charge for customer data transfers

Transfers of customer-provided and transaction data should be provided free of charge.

Recommendation 3.12 – transfers of identity verification assessment outcomes

Provided that the liability borne by the original verifying entity does not multiply as the outcomes of identity verification assessments are shared through the system, those outcomes should be provided without charge.

Chapter 4: Safeguards to inspire confidence

Recommendation 4.1 – application of the Privacy Act

Data recipients under Open Banking must be subject to the Privacy Act.

Recommendation 4.2 – modifications to privacy protections

The privacy protections applicable to Open Banking should be modified as suggested in Table 4.1.

Recommendation 4.3 – right to delete

Given the many complexities involved in legislating for a right to deletion (including the range of legal obligations to retain records) and the fact that individuals currently have no right to instruct deletion of their personal information under the Privacy Act, it is beyond the scope of Open Banking to mandate a special right to deletion of information.

Recommendation 4.4 – dispute resolution for small business

Small business customers should be given access to internal and external dispute resolution services for confidentiality disputes similar to those that exist for individuals under the Privacy Act.

Recommendation 4.5 – customer control

A customer's consent under Open Banking must be explicit, fully informed and able to be permitted or constrained according to the customer's instructions.

Recommendation 4.6 – single screen notification

A data holder should notify the customer that their direction has been received and that the future use of the data by the data recipient will be at the customer's own risk. That notification should be limited to a single screen or page. Data recipients should similarly provide the customer with a single screen or page summarising the possible uses to which their data could be put and allow customers to self-select the uses they agree to.

Recommendation 4.7 – joint accounts

Authorisation for transfers of data relating to a joint account should reflect the authorisations for transfers of money from the joint account. Each joint account holder should be notified of any data transfer arrangements initiated on their accounts and given the ability to readily terminate any data sharing arrangements initiated by any other joint account holders.

Recommendation 4.8 – security standards

In order to be accredited to participate in Open Banking, all parties must comply with designated security standards set by the Data Standards Body.

Recommendation 4.9 – allocation of liability

A clear and comprehensive framework for the allocation of liability between participants in Open Banking should be implemented. This framework should make it clear that participants in Open Banking are liable for their own conduct, but not the conduct of other participants. To the extent possible, the liability framework should be consistent with existing legal frameworks to ensure that there is no uncertainty about the rights of customers or liability of data holders.

Chapter 5: The data transfer mechanism

Recommendation 5.1 – application programming interfaces

Data holders should be required to allow customers to share information with eligible parties via a dedicated application programming interface (API).

Recommendation 5.2 – starting point for the data transfer Standards

The starting point for the Standards for the data transfer mechanism should be the UK Open Banking technical specification. The specification should not be adopted without appropriate consideration, but the onus should be on those who wish to make changes.

Recommendation 5.3 – extensibility

The Data Standards Body should start with the core requirements, but ensure extensibility for future functionality.

Recommendation 5.4 – customer-friendly authentication and authorisation

The redirect-based authorisation and authentication flow detailed in the UK technical specification should be the starting point. Consideration should be given to the merits of a decoupled approach provided it minimises customer friction.

Recommendation 5.5 – no additional barriers to authorisation

Data holders may not add authorisation requirements beyond those included in the Standards. Requiring multifactor authentication is a reasonable additional security measure, but it must be consistent with the authentication requirements applied in direct interactions between the data holder and its customers.

Recommendation 5.6 – persistent authorisation

Customers should be able to grant persistent authorisation. They should also be able to limit the authorisation period at their discretion, revoke authorisation through the third-party service or via the data holder and be notified periodically they are still sharing their information. All authorisations should expire after a set period.

Recommendation 5.7 – access to rich data

Customers should be able to authorise access to transaction data in full. Data recipients should not be limited to accessing pre-set functions or sending blocks of their own code to run on the system of the bank or its partner or prevented from caching data. However, participants should be free to offer services that provide more limited data to data recipients who have lower levels of accreditation.

Recommendation 5.8 – intermediaries

The Standards should allow for delegation of access to intermediaries such as middleware providers.

Recommendation 5.9 – access without online banking

The Standards should allow users who do not use online banking to authorise the sharing of information through service channels which are ordinarily provided by the data holder.

Recommendation 5.10 – access frequency

The Data Standards Body should determine how to limit the number of data requests that can be made.

Recommendation 5.11 – transparency

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.

Chapter 6: Implementation and beyond

Recommendation 6.1 – the Open Banking Commencement Date

A period of approximately 12 months between the announcement of a final Government decision on Open Banking and the Commencement Date should be allowed for implementation.

Recommendation 6.2 – phased commencement for entities

From the Commencement Date, the four major Australian banks should be obliged to comply with a direction to share data under Open Banking. The remaining Authorised Deposit-taking Institutions should be obliged to share data from 12 months after the Commencement Date, unless the ACCC determines that a later date is more appropriate.

Recommendation 6.3 – commencement date for data

From the Commencement Date, Open Banking should apply to transaction data and product data. However, Open Banking should not apply to transaction data relating to transactions before 1 January 2017. Open Banking should apply to customer-provided data and the outcomes of identity verification assessments on a date to be determined by the ACCC.

Recommendation 6.4 – consumer education programme

The ACCC as lead regulator should coordinate 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.

Recommendation 6.5 – the appropriate funding model

As banking is the first sector to which a much broader Consumer Data Right will apply, it would be difficult to impose an industry-funded model to cover regulatory costs at the outset. Neither the total costs, nor the number of sectors or participants will be known for some time, so it would be impossible to make an estimate of the average cost until the system is well-established. The funding arrangement could be reconsidered after a period of operation, when there is a more refined cost structure and greater certainty over the number of participants.

Recommendation 6.6 – timely post-implementation assessment

A post-implementation assessment of Open Banking should be conducted by the regulator (or an independent person) approximately 12 months after the Commencement Date and report to the Minister with recommendations.

Chapter 1: Context for the Review

Giving customers greater access to and control over their banking data has the potential to transform the way in which they use and benefit from the banking system.[2]

There is substantial value in customers' banking data. It can give insights into a customer's financial situation, how they manage their finances, where they spend their money and how they use financial services. To date, the value in that data has been largely captured by the banks that hold it. Open Banking aims to give customers the ability to use that value for their own benefit.

Under Open Banking, the holders of banking data (i.e. banks) will be obliged to securely share a customer's banking data, at the customer's direction and with parties nominated by the customer, in a form that facilitates its use. These parties might include, for instance:

- competing providers of banking and financial services striving to offer a better deal for the customer
- comparator services that can identify which banking products and services best meet the customer's needs, and
- providers of tools to help a customer better manage their finances or tax affairs.

The Review into Open Banking in Australia

In the 2017-18 Budget the Government announced it would introduce an Open Banking regime in Australia and commissioned a review to provide advice on its design and implementation. On 20 July 2017, the Treasurer, the Hon Scott Morrison MP, announced the Terms of Reference[3] and appointed Mr Scott Farrell to lead the Review.

The Review was asked to make recommendations to the Treasurer on:

- the most appropriate model for the operation of Open Banking in the Australian context, including the advantages and disadvantages of different data-sharing models
- a regulatory framework under which an Open Banking system would operate and the necessary instruments (such as legislation) required to support and enforce a system, and
- an implementation framework (including roadmap and timeframe) and the ongoing role for the Government in implementing an Open Banking system.

These recommendations required an examination of:

- the scope of the data sets to be shared, the parties who will be required to share, and to whom the data sets may be provided in specified circumstances

2. Treasurer's media release, 20 July 2017. Available at: http://sjm.ministers.treasury.gov.au/media-release/065-2017/
3. See Appendix A for the Review's full Terms of Reference.

- existing and potential technical data transfer mechanisms for sharing relevant data (and existing or potential sector standards) including customer consent mechanisms
- the key issues and risks, such as customer usability and confidence, security of data, privacy safeguard requirements, liability for breaches arising from the adoption of potential data transfer mechanisms and the enforcement of customer rights, and
- the costs of implementation of an Open Banking system and the means by which costs may be recovered, including consideration of industry-funded models.

The Review was requested to have regard to:

- the Productivity Commission's final report on *Data Availability and Use* and any government response to that report
- best practice developments internationally and in other industry sectors, and
- competition, fairness, innovation, efficiency, regulatory compliance costs and consumer protection in the financial system.

Consistent with these Terms of Reference[4] this Report makes recommendations on:

- the regulatory framework needed to give effect to and administer the regime
- how to ensure shared data is kept secure and privacy is respected
- what data should be shared, by whom and with whom
- how data should be shared, and
- a roadmap and timetable for implementation of the Review's recommendations in order to deliver Open Banking in a timely way.

The Review notes that payment initiation (also known as 'write access') was not part of its Terms of Reference and so has not been considered in this Report to be part of the initial scope of Open Banking in Australia.

This report makes 50 recommendations in total. Implemented sensibly, these recommendations should produce a dynamic, secure and sustainable Open Banking system to enhance competition and innovation in the banking sector for the benefit of customers and the broader economy.

Policy context

The Treasurer's 2017-18 Budget announcement followed a number of reviews and inquiries that have recommended expanding customers' access to data.

The 2014 Financial System Inquiry (the Murray Inquiry) recognised the role that increased data sharing could play in the development of alternative business models and products and services of the type that will improve consumer outcomes in financial services. It argued for the development of

4. Terms of Reference are at Appendix A.

standards for accessing and formatting data and product information, which also addressed consumer privacy concerns to strengthen confidence and trust in the use of data.

Similarly, the 2015 Competition Policy Review (the Harper Review) recommended that the Government consider ways to improve individuals' ability to access their own data to inform customer choices.

In 2016 the Report of the House of Representatives Standing Committee on Economics' Review of the Four Major Banks (the Coleman Report) concluded that there was a strong case for increasing consumers' access to their banking data and to banking product data. The Committee recommended that banks be required to provide open access to customer and small business data by July 2018.

To develop these ideas further, the Government commissioned the PC's Data Report. The PC's Data Report, released in May 2017, proposed a significant set of reforms, including the creation of a new economy-wide Comprehensive Right to Data to give individuals and small-to-medium businesses greater access to their data.

In November 2017, the Government formally responded to the PC Data Report. In its response, the Government announced that it will introduce a Consumer Data Right to allow individuals and small-to-medium businesses to access particular data, including transaction and product usage data, in a useful digital format. Consumers will also be able to direct a business to transfer that data to a third party. Implementation of the Consumer Data Right will be prioritised in the banking, energy and telecommunications sectors, before being rolled to other industry sectors over time.

Against this background the Review has approached its task on the basis that banking would be an early implementation of broader reforms granting consumers easier access to data in multiple sectors. Nothing the Review has been presented with showed any compelling reason why the banking sector could not be regulated by a framework that can also apply to other industries, provided each sectors' relative risks are assessed and the system design allows adjustment for each. Moreover, it appears likely that the benefits of customer-driven transfer of data across industries into the future may far exceed that of Open Banking itself. The Government has announced that banking will be the first sector to be designated under the Consumer Data Right.

The potential benefits of a data sharing system are not limited to participants in the banking industry. As addressed in the PC Data Report, the opportunities for greater customer information and choice abound in a range of industries. While the potential gains from enabling customers to share their banking data are significant, banking is far from the only industry that could potentially benefit from a framework regulating customers' rights to the access and transfer data.

Data sharing in banking – current state of play

Australian banks currently engage in data sharing with partner companies frequently, typically through negotiated bilateral agreements. One of the most common agreements is that between a bank and a credit bureau, for the purposes of assessing the creditworthiness of current or prospective customers. At the time of application for credit, banks seek customers' consent to allow this data sharing to occur in accordance with Australian privacy law. Banks also have arrangements with accounting software providers to help their customers manage their accounting needs.

In recent years, a number of FinTech companies have emerged with business models that rely on so-called 'screenscraping' technology to access customers' data from their existing banking accounts. Screenscraping involves allowing third parties to access a customer's bank account using the customer's access credentials (such as their internet banking username and password).[5]

Some Australian banks have announced initiatives, or intentions, to increase data sharing. To date, these initiatives have largely involved the opening up of limited, non-customer, data sets to software developers and FinTech companies — such as data on branch and ATM locations, and on foreign exchange rates. More recently, one large bank announced the establishment of an Open Banking platform that would allow its customers to initiate a request to securely move their data to third party participants that have been approved to be part of the platform.

Over the course of the Review several banks have indicated that they see greater potential value in increased data sharing for both their customers and their own business. However, given the competitive advantages afforded to large incumbent firms by limiting the ability of customers to share their data with third parties, these initiatives alone seem unlikely to lead to a widespread increase in data sharing across the banking sector.

Consultation process

The Review released an Issues Paper on 9 August 2017, inviting interested parties to provide their views over six weeks on aspects of the issues raised in the Issues Paper, or any other matters they felt were relevant.

The Review attracted a wide range of interest, with a total of 41 submissions received from:

- banks
- FinTech businesses
- industry bodies
- consumer advocates
- credit bureaux
- payments services providers and credit card schemes
- law firms
- regulators and other government agencies, and
- private individuals.

The Review also engaged with interested parties through large roundtable discussions, small group and bilateral discussions. Large roundtable meetings were held in Sydney on 9 October 2017 and Melbourne on 20 October 2017. A targeted roundtable discussion with consumer groups and privacy advocates was held in Canberra on 28 November 2017. The Review has held more than 100 other meetings with representatives from across the spectrum of interested parties. To gain insights from

5. See Box 5.2 in Chapter 5.

other countries' experiences, discussions were also held with policy makers, regulators and entities involved in Open Banking initiatives in overseas jurisdictions.[6]

Submissions to the Review overwhelmingly supported the introduction of Open Banking in Australia as a means to deliver greater choice and better outcomes for customers, with a large number emphasising the importance of placing customers' interests at the centre of its development. There were, however, differences of opinion as to how Open Banking should be implemented.

While some submissions argued that Open Banking should be very broad in its application, and start as soon as possible, others recommended that, at least in its initial phase, it should be applied to a relatively narrow set of data types and participants, or based on specific 'use cases'. (A use case is where a particular data set has a current and demonstrable application to the provision of a financial product or service.) Targeting modest gains in the initial implementation phase would, it was argued, help build customer confidence in data sharing and give industry the time to put in place the necessary capabilities to respond to customer data sharing requests. Some submitters also argued that a tentative approach to the introduction of Open Banking was an appropriate first step given the future rollout of the economy-wide data sharing model advocated by the PC Data Report.

There was broad agreement that protecting the privacy and security of customers' banking data was vital to the success of Open Banking and that only entities meeting required standards should be allowed to participate. However, there was less consensus on the standards that accredited entities should be required to meet. Some argued that increasing cyber-crime and the sensitive nature of banking data meant accredited entities should meet security standards commensurate with those of banks. Others thought that requiring smaller participants to meet the banks' security standards would be a significant barrier to entry into the system. Banks' standards were understandably higher, some argued, as they protected money itself, not just information about money. There were also differing views as to who should perform the accreditation role — with some advocating a regulator-led process and others proposing an industry-led accreditation utility.

Partly, this divergence of views reflects different perceptions of what the scope of Open Banking might be, and therefore differing views about the security and privacy risks. Some submissions argued that more widespread data sharing would significantly increase the risk of security and privacy breaches of customer data. Others believed that the widely accepted (and accessible) international standards for managing data security risks could be readily adopted in the Australian context, and that appropriate safeguards – including an explicit and express direction and consent framework – could manage privacy risks. Some also observed that a large number of Australian customers are currently taking significant risks by providing their bank login credentials to companies that 'screenscrape' their banking data and that Open Banking promises a far more secure way of sharing data than screenscraping. Privacy advocates argued that Australia's existing privacy laws needed significant upgrading in order to provide adequate protections for consumers.
While acknowledging that better access to banking data had the potential to improve consumer outcomes in banking, consumer groups' initial submissions cautioned that robust legal and regulatory safeguards were required.

6. For a summary of Open Banking initiatives overseas, see Appendix C.

While there was general agreement on the appropriate technology solutions for enabling data sharing under Open Banking, there was less agreement on how prescriptive the standards defining data sharing should be and the process by which any standards should be set. Some submissions suggested that prescriptive standards for data sharing were not needed because the technological challenges involved in translating data between institutions with different systems were not insurmountable. Others thought that the absence of defined standards would act as a significant barrier to entry for smaller institutions and therefore jeopardise the ability of Open Banking to deliver innovative services to customers. Some submissions advocated for an industry-led process for developing standards, while others argued that the Government and regulators should play a central role in setting standards.

On the appropriate regulatory model, many pointed to the economy-wide Consumer Data Right proposed by the PC's Data Report and argued that Open Banking should be pursued as part of that broader reform. A point of difference between submissions was whether Open Banking should be implemented under a competition, privacy or perhaps even a financial services legislative framework. Submissions advocating a competition approach argued that, given the competition objectives, competition law was the appropriate regulatory lens through which to approach Open Banking. Others took the view that a joint regulatory model, overseen by both the competition regulator (i.e. the ACCC) and the privacy regulator (i.e. the OAIC) would be sensible. Those advocating implementation under financial services law argued that the existing Australian Financial Services Licence (AFSL) regime administered by ASIC provided an appropriate legislative basis for Open Banking.

The potential of Open Banking

An accumulation of evidence suggests that many Australian consumers and businesses could be getting a better deal on banking. Customers tend to remain with the same banking services provider for extended periods, even in the presence of more competitive offerings elsewhere. A persistent theme in findings of poor customer outcomes is the role played by poor availability of meaningful information.

For customers, it can be a complex task to differentiate between available banking products to determine which best suits their needs. Faced with this complexity, many customers base their decisions on rules of thumb or shortcuts — such as following what their peers have done, choosing a well-known institution, or choosing an institution with which they already have a banking relationship. In some cases, such decision-making processes can result in reasonable customer outcomes. In others, they can have a substantial, detrimental impact on individuals' long term financial outcomes.

For competing providers and new market entrants, their ability to attract customers away from incumbent firms is hampered by their ability to efficiently and accurately assess the suitability of

potential customers. This places them at a significant competitive disadvantage to incumbent firms that are able to use data they hold on their customers largely for their exclusive benefit.[7]

These so-called 'information asymmetries' are a pervasive feature of banking and financial markets. Standard economic theory, and a range of corroborating empirical evidence, suggests that markets work most efficiently when: customers are informed; there is transparency in pricing and in the quality of available products and services; there is a level playing field between competitors; and where the costs of switching between providers and barriers to entry for new providers are low.

At its most fundamental level, Open Banking seeks to reduce those barriers. Requiring banks to grant open access to data on their product terms and conditions while giving customers the ability to direct their bank to securely share their banking data with whom they choose, should lead to the development of comparison services better able to provide tailored product recommendations. Better tailored product recommendations could dramatically simplify the choices faced by customers when accessing financial services. And giving customers the ability to transfer their data to a new provider will help to overcome the 'hassle factor' that sees customers stick with their current provider even in the presence of more competitive deals elsewhere.

Open Banking could lead to the development of new financial products and services for specific customer groups, such as the significant minority of Australians that are classified as financially excluded or those with unstable incomes.[8] The causes of financial exclusion are varied and include factors such as the cost of basic financial products, poor credit ratings or a lack of basic financial literacy. Increased data sharing will open opportunities for financial services providers to pool available information on financially excluded customers, enabling them to get a more complete picture of customers' financial situation and develop products and services that are better tailored to their needs.[9]

For competing providers of banking services (including new market entrants), having access to customers' banking data in a form that facilitates its transfer and use can enhance their ability to assess potential customers. It can also enable new and competing providers to better tailor their products to a customer's specific needs and at a more competitive price. It can open up opportunities to develop new products and services — either 'in-house' or in collaboration with third parties — to increase their value proposition and create additional revenue streams.

For small business customers, the ability to instruct their banking services provider to share their data with competing providers and other third parties could open up a new era of competition in banking. Information asymmetries in small business banking tend to be more acute and present

7. For incumbent firms, there are many potential uses of customers' banking data. They can use it to draw insights into the creditworthiness, preferences and needs of their customers. It can also allow incumbent firms to develop new forms of targeted marketing (by suggesting new products based on an individual's circumstances), or to provide forward-looking financial advice.
8. Financial exclusion exists where individuals lack access to appropriate and affordable financial services and products. The Centre for Social Impact, in cooperation with NAB, has estimated that 16.9 per cent of the Australian adult population were either totally excluded (1 per cent) or severely excluded (15.9 per cent) from financial services. They define financial exclusion as an inability to access appropriate and affordable financial services and products, including access to a moderate amount of credit.
9. However, the joint submission from Consumer Action Law Centre, Financial Rights Legal Centre and Financial Counselling Australia also identified concerns regarding consumer profiling, predatory practices and the potential for Open Banking to be used to unfairly discriminate against those that are financially excluded.

more significant barriers to competition than in other customer segments. Smaller businesses typically have less documentation and shorter financial histories. This makes it generally harder and more costly for banks to acquire the required information to make accurate assessments of small businesses' creditworthiness.[10] Giving competing providers access to data on potential small business customers would allow them to make such assessments more easily and cheaply, leading to more competitive prices for small business customers.

Guiding principles for the Review

In some respects, Open Banking is a simple concept – it is about giving customers the ability to instruct that their banking data be securely shared with parties they trust to unlock the value in that data. Practically, however, Open Banking raises many complex issues that this Review has been tasked with providing solutions to.

In examining the issues, the Review has adopted the approach that the framework must support the creation and maintenance of a system that:

- is customer focussed
- promotes competition
- encourages innovation, and
- is efficient and fair.

In addition to these principles, the Review also considers that the system should allow for alternative approaches.

Some implications of those principles are set out below.

Customer focussed

To ensure that Open Banking is customer focussed, it should promote a well-designed customer experience. A well-designed customer experience means that data transfers and use are driven by customers' informed choice (and at their express direction) and that customers have access to a practical means to resolve problems.

An important component of this customer focus is that all participants feel justifiably confident in the system. Customers and other participants will not engage with a system that they do not trust. Trust includes knowing that customer data will remain protected, that any breach will be remedied, and that a system customers have integrated into their lives will remain stable and accessible.

10. The RBA has found that the market for small business loans, for example, has more structural impediments to competition than most other lending markets because the information asymmetries tend to be more significant (RBA FSI submission, page 154). Banks have to invest resources to acquire sufficient information to make a well-informed lending decision, which increases the cost of assessing and approving a loan application. When lenders are unable to access sufficient information to make a proper assessment, the risks associated with the loan are generally, and justifiably, perceived to be greater. This leads to higher provisioning and higher loan costs for the borrower (FSI Interim Report).

For customers to be confident in the system they must be in control of their own information. Data transfer must only ever occur within the authorisations actively chosen by the customer. All aspects of the Open Banking system should be transparent — to customers, participants and regulators.

For Open Banking to achieve this customer focus, the customers' voices need to be heard through customer engagement in its design and implementation.

Promotes competition

Open Banking is intended to provide customers with choices and support firms who want to provide better products and services to reach customers. Open Banking should not unreasonably lock out new participants and should not place unreasonable costs on existing participants. In providing customers with greater choice, Open Banking needs to be capable of balancing the needs of different participants to ensure that the system is fair to everyone.

Open Banking also needs to allow participants to connect to each other — this requires adequate specification of how participants connect. Industry and technical experience and expertise should be drawn upon to prevent technology becoming a barrier to entry.

Encourages innovation

Many customer benefits should come from new products and services that are currently unable to be foreseen. From the range of submissions received, we know that these opportunities may include: product comparison services that simplify the range of choices available to customers by providing tailored options; safe data storage and amalgamation; and budgeting tools to help customers better manage their finances. The pace at which these innovations occur and are adopted is likely to be hastened by the introduction of Open Banking.

To enable innovation Open Banking needs to be flexible, future oriented and responsive to change. We know that technology is going to improve and what is the best solution now will not be the best solution in the future. To incorporate these future solutions, Open Banking needs to be capable of implementing relatively rapid change, in a manner that allows participants to adjust.

Efficient and fair

Market forces are the primary driver of good customer outcomes, while the role of regulation is to address failures by the market to achieve this. Where regulation is required it should first seek to assist market forces, only seeking to replace them when there is no other suitable alternative. As such, Open Banking should only do as much as is necessary to support industry-driven development of a system that meets the needs of customers.

High regulatory costs would have a profound impact on innovation and would create significant barriers to entry to new participants. If the regulatory burden associated with Open Banking is too high, non-mandated companies may lack the incentive to participate and the policy will fail to achieve its objectives.

It is not sufficient, however, to create a Consumer Data Right without creating the regulatory infrastructure to support that right. If customers are unaware that they have this right, or if they feel

insufficiently protected in exercising that right, customers may lack the incentive to participate. Open Banking must therefore balance these competing interests and incentives so that it is implementable for all prospective participants.

Allows for competing approaches

Finally, while the Review has been tasked with recommending a regulatory framework to 'support and enforce [an Open Banking] regime', Open Banking should not be the only way that banking data may be shared. Alternative data sharing methods already exist and new ones will inevitably emerge — closing those off would unnecessarily constrain future innovation.

Moreover, allowing competing approaches will provide an important benchmark against which to judge the success of Open Banking. Should those competing approaches become more actively used than those specified under Open Banking, this will provide a valuable signal to regulatory authorities that the design of Open Banking may need to be revisited.

Recommendation 1.1 – allowing for competing approaches

Open Banking should not be mandated as the only way that banking data may be shared. Allowing competing approaches will provide an important test of the design quality of Open Banking and the Consumer Data Right.

Chapter 2: Open Banking regulatory framework

The structure of the regulatory framework

This chapter sets out recommendations about the regulatory framework for Open Banking. The Review has been tasked with recommending 'a regulatory framework under which an open banking regime would operate and the necessary instruments (such as legislation) required to support and enforce a regime'.[11] As banking is the first sector that the Consumer Data Right (CDR) will apply to, this chapter recommends a regulatory framework that allows Open Banking to be implemented smoothly and that can be applied to other sectors.

In the Productivity Commission's Data Availability and Use Inquiry (PC Data Report), the Productivity Commission (PC) recommended that an economy-wide Comprehensive Right to Data should be created in a new Data Sharing and Release Act. The PC recommended that this Act should replicate elements of the *Privacy Act 1988* (Privacy Act), and incorporate the other recommendations of the PC Data Report, including the creation of a National Data Custodian. In alignment with its objective that Open Banking be efficient, this Review considered that the creation of a new Act was not needed. Such an undertaking would be a major project, taking considerable time and, if rushed, could introduce a risk of error and unintended consequences.

For simplicity, and ease of implementation, the Review has recommended a design that minimises duplication of existing legislation. This design uses existing privacy, confidentiality laws, plus consumer and competition principles operating together, and requires new legislation only to fill any regulatory gaps.

It is important that the regulatory framework for the CDR is able to apply beyond banking and across other sectors, including the energy and telecommunications sectors. The right hierarchy of regulations (using legislation, subsidiary legislative instruments and non-binding guidance such as standards) needs to be chosen. In practice, this means assigning the necessary rule-making functions to the right level and devolving decision-making where quicker responses may be required.

As *legislation* is typically hard to change, it should contain only those ideas and principles that are intended to last. The legislation implementing the overarching CDR should therefore be outcomes-based, capable of applying to the entire economy. It should establish a Ministerial power to apply the CDR to designated sectors and data-sets (with Open Banking being the first such designation) and set the parameters for subsidiary rule-making.

Subsidiary instruments (ministerial determinations, regulations and other legislative instruments) can respond more quickly to technological change and are therefore better suited for more in-depth rules that may change more often. Once a sector is designated by the Minister (which would occur under a ministerial determination), rules (the Rules) will be needed to set expectations of what the

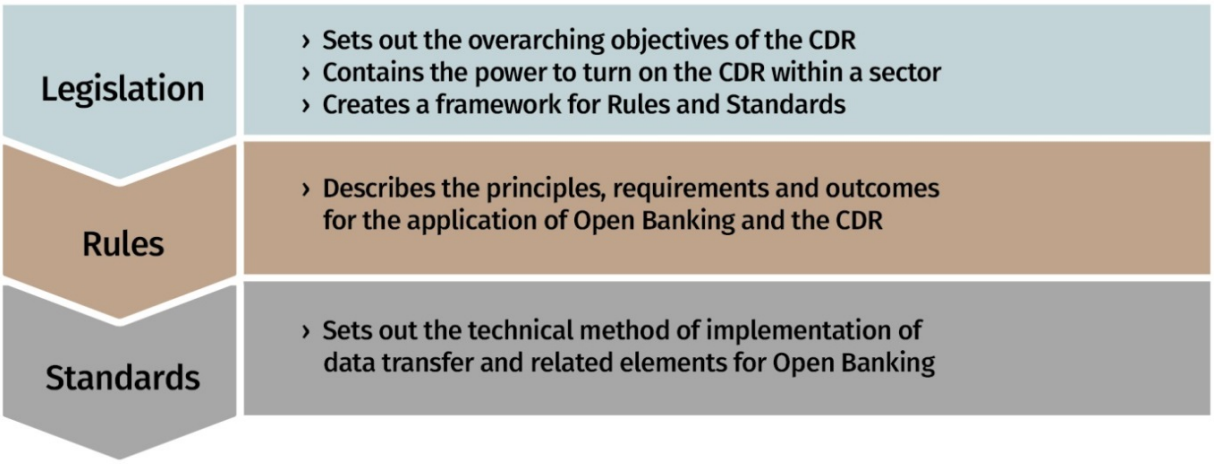
11. See Terms of Reference at Appendix A.

CDR system for each sector must deliver and determine how those expectations are met. The rights between the designated sectors need to interact efficiently. Accordingly, Government should provide leadership — 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.

Finally, as the regulatory framework will apply to technology, *standards* (the Standards) may be required. These Standards should set a base-line for the technical components of the relevant sector's CDR system (such as Open Banking, in the case of the banking sector), but should not otherwise impede innovation or competition. The Standards may need to change quickly as technology develops. Standards make implementation cheaper, more efficient, and can simplify compliance with the Rules. While these Standards could be allowed to evolve naturally over time,[12] the fact that the Government is mandating participation requires a certain level of intervention. This intervention is to prevent the use of technology as a barrier to participation, and increase efficiency in the system by overcoming the need for parties to negotiate bilaterally. The challenge for Government is to prescribe only those things that data holders[13] and developers will find necessary to participate, while not attempting to 'pick winners' in terms of technology or business models.

In summary, the Review has concluded that a regulatory framework that assigns decision-making to the appropriate level would allow the concepts underlying Open Banking to be implementable over time and adaptable across sectors, consistent with other elements of the CDR. Figure 2.1 illustrates the decision-making hierarchy for regulating the CDR, starting with Open Banking.

Figure 2.1: A hierarchy of legislative instruments

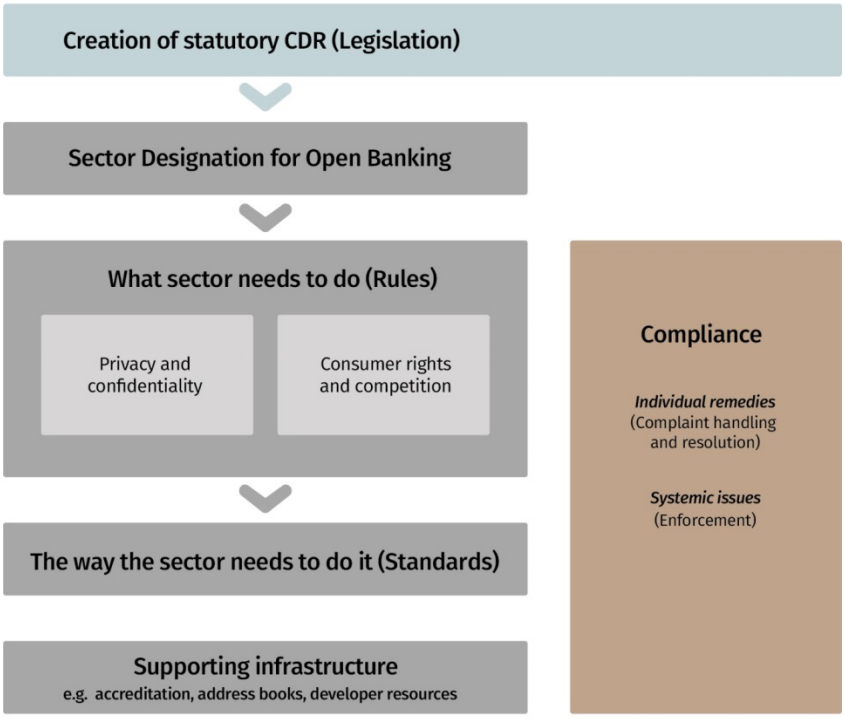


12. As have internet standards, for example.
13. The Review has chosen to depart from UK Open Banking definitions of participants as industry engagement has suggested that these definitions may not cover all roles that may develop in a data transfer system. See the Glossary for definitions used in this Review.

The regulatory elements of Open Banking

In addition to legislation, Rules and Standards, the regulatory framework will need to incorporate: the power to apply the CDR to sectors; compliance requirements including complaints handling and enforcement; and provision of supporting infrastructure including accreditation, address books, and developer resources. When examining each element, it is important to consider how it works as a part of the whole. Figure 2.2 below illustrates how these elements interact.[14]

Figure 2.2: Elements of the Regulatory framework



The legislation

The primary reason for Open Banking and the CDR is to benefit customers by providing the tools to enable them to make informed choices. The legislative framework therefore needs to be customer focussed and allow customers to engage as active participants, while protecting their privacy.

As Open Banking is a starting point for a broader right, whatever is implemented as part of Open Banking should be implementable across other sectors over time. To achieve this efficiently, the right needs to originate in legislation that applies throughout the economy, and be applied to sectors as required. For this reason, implementation of Open Banking through banking sector specific instruments in the *Australian Securities and Investments Commission Act 2001*, or the *Corporations Act 2001*, or through changes to existing licensing requirements, would not be optimal.

14. A more detailed explanation can be found in Appendix D.

In regulating for the CDR, the Government is effectively facilitating the emerging data transfer system, and intending to do this safely and securely. Balancing system function and customer protection results in a tension between measures designed to share information and measures designed to keep information private. Many aspects of the regulatory framework that may be designed to protect customers could be used in anti-competitive ways if that balance is wrong. In navigating this tension, a focus on the customer is essential. The CDR should therefore be implemented in an Act that encourages a culture that focuses on the customer and the customer's choice. As discussed in depth below, the Privacy Act alone would not be a suitable regulatory framework to achieve these aims.[15] The most prominent existing legislative framework that promotes decision-making in a customer and competition based framework, with a regulator that has experience and expertise in market regulation, is the *Competition and Consumer Act 2010* (CCA).

Applying the regulatory framework explained earlier, the CCA should be amended to include principles-based legislation focussed on the objectives and outcomes to be achieved through the CDR. The CCA could provide for sectors to be designated, describe what the Rules should cover, and allow for the sector-focussed Rules to be specified in subsidiary instruments. For certainty, amendments to the CCA should also address intellectual property considerations and create rights (such as the right for accredited entities to participate) and liabilities (such as liability for breaches of the Rules).

Recommendation 2.1 – a layered regulatory approach

Open Banking should be implemented primarily through amendments to the *Competition and Consumer Act 2010* that set out the overarching objectives of the Consumer Data Right. The amendments should enable the designation of a sector by Ministerial direction and create the power to set out regulations and operational Rules for sectors. This structure will embed a customer and competition focus in Open Banking, while allowing the Consumer Data Right to be scalable across sectors.

The regulators

To discuss the next level of legislative instruments dealing with requirements for designated sectors, it is necessary to discuss the regulators that may be called upon to set them. There are two key regulators to consider, the Office of the Australian Information Commissioner (OAIC), with privacy responsibilities, and the Australian Competition and Consumer Commission (ACCC), with responsibility for competition and consumer issues.

The Office of the Australian Information Commissioner

Many submissions argued that independent and accountable regulators with clear roles and responsibilities are necessary to maintain trust and confidence in Open Banking.[16]

15. Under the heading *Access to personal information under APP 12.*
16. See for example, NAB submission, page 15 and ABA submission, page 5.

The OAIC submitted that Open Banking should be implemented with small changes to the Privacy Act and the OAIC as sole or primary regulator.[17] The OAIC argued that the functions of privacy, freedom of information, and Government information management, combined with experience of regulating the *Privacy (Credit Reporting) Code 2014* meant that 'the OAIC is well placed to strike the right balance between confidentiality and transparency' and that this approach would avoid unnecessary duplication and complexity.[18] The OAIC proposal relies on the existing right to request personal information under Australian Privacy Principle 12 (APP 12).

Access to personal information under APP 12

APP 12 provides a framework for giving individuals access to their personal information by setting out how access is to be given and when access can be refused. APP 12 allows an entity to impose fees in relation to the provision of access but those fees must not be excessive. Individuals are able to request their data be provided to them in a particular form and allow the request for information to come from an authorised agent.

Given the parallels and likely overlaps with the rights available under APP 12, the suitability of APP 12 as the mechanism to allow a customer to access or share their own data needs to be examined. The Financial System Inquiry (FSI) considered this issue when reviewing the costs and benefits of increasing access to and improving the use of data in the financial sector. The FSI expressed concerns that customers are not readily utilising the Privacy Act to access personal information about themselves and that a number of impediments exist to customers using their personal information effectively. The FSI noted that one of these impediments is that customers are unable to authorise trusted parties to access their personal information directly from their service provider. Lack of access to this information reduces the ability of competitors to offer customers better value or tailored services, or develop advice services to better inform customer decision-making.

As for all APPs, APP 12 is limited in its application to individuals (as opposed to businesses) given the Privacy Act only applies to personal information. Open Banking and the CDR is not limited to individual customers.[19]

APP 12 permits a request for access to information to come from a third party. However, the recipient must be an authorised agent of the individual. The Review considers that an agency relationship between the customer and a data recipient is not necessary under Open Banking. An agency relationship would raise unnecessary complications regarding the liability and range of legal remedies under common law and equity if the data recipient breaches their obligations.

APP 12 also provides a number of grounds for refusing access to personal information.[20] These grounds will need to be adjusted considerably to apply effectively to Open Banking. In addition, the

17. OAIC submission, page 6.
18. OAIC submission, page 2.
19. See discussion of scope in Chapter 3.
20. These grounds include: access would pose a serious threat to the life, health or safety of any individual; have an unreasonable impact on the privacy of other individuals; is frivolous or vexatious; relates to existing or anticipated legal proceedings; would reveal the intentions of the organisation in relation to negotiations; access would be unlawful; denying access is required by law; the organisation has reason to suspect unlawful activity or misconduct of a serious nature; giving access would be likely to prejudice one of more enforcement related activities; or giving access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process.

timeframe for responding to a request, the ability to apply access charges and the form in which the personal information is to be provided would need to be altered.

As submitted by FinTech Australia, issues with extending the Privacy Act for this purpose include:

> *… the current law is limited around [consumers'] ability to control [their personal financial data], for example their ability to limit the time period (e.g. once off, one month, ongoing until told to stop), and in placing obligations on an entity currently holding the desired financial data to share this with a third party if the consumer directs them to do so. It is also not currently explicit in the APPs that this control and consent framework should extend to small businesses.*[21]

Fundamentally, the CDR is a right to direct information be shared in a manner that is useful to the recipient (in order to meet the needs of the customer). Framing such a right solely through a privacy lens is likely to place undue emphasis on privacy at the expense of efficiency through competition.

Having examined this approach, the Review considers that the amendments that would be required to the Privacy Act to implement the breadth of the CDR would not be minor. Significant adjustments would be required, as the Privacy Act does not provide protections for non-individuals, does not make liability for loss clear, or bind small businesses as data holders. Perhaps most importantly, it has no clear competition-enhancing objectives.[22]

The Review considers that extending the role of the OAIC beyond privacy protection, freedom of information and Government information management functions for the purpose of Open Banking risks complicating the remit of the Information Commissioner. Were this proposal adopted, it could impair the competition-enhancing goals of the Open Banking system. Nevertheless, a clearly focussed, accountable privacy advocate is a necessary element in a customer directed data transfer system. The Review considers that it is important for the OAIC to continue to perform this privacy protection role in the Open Banking and CDR context.

A multiple regulator model

Several regulators are currently involved in regulating banking. The Australian Prudential Regulation Authority (APRA) is the prudential regulator of the Australian financial services industry.
The Australian Securities and Investments Commission (ASIC) regulates the conduct of financial service and consumer credit providers and assesses how effectively authorised financial markets are complying with their legal obligations. The Reserve Bank of Australia (RBA) fosters financial system stability and is the primary regulator of the payments system. The ACCC protects and supplements the way competition works in Australian markets and industries, including financial markets.
The OAIC protects the privacy of individuals and handles privacy complaints.

As a result, a dual or multiple regulator model may be the best vehicle to both protect customers and provide them with access to new opportunities and choices. Such a model would minimally disrupt current arrangements, provided respective regulatory roles are clear.

---

21. FinTech Australia submission, page 32.
22. See section 2A of the *Privacy Act 1988* for the objects of the Act.

A partnership of regulators would have the ACCC as the lead (having responsibility for the CDR as a whole and competition and customer outcomes in particular), and the OAIC having primary responsibility for privacy protection (as is their current role). Under an effective regulatory framework, the ACCC would work closely with the OAIC to minimise duplication in the roles and responsibilities of the two regulators. Conceptually, the regulator model could be similar to the relationship between the Australian Communications and Media Authority (ACMA) and the OAIC under the *Telecommunications Act 1997*. The UK has adopted a similar model. The Competition and Markets Authority (CMA) issued an order requiring implementation of Open Banking, the Financial Conduct Authority (FCA) sets requirements, and the Information Commissioner's Office retains responsibility for data and privacy protection.

The ACCC's additional responsibilities should include powers to undertake sector assessments, make rules setting out expectations, accredit parties, oversee specifications, and enforce systemic issues. The ACCC would consult with the relevant sector-focussed regulators when necessary. In the case of banking, this would include ASIC, APRA and the RBA. 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).

Recommendation 2.2 – the regulator model

Open Banking should be supported by a multiple regulator model, led by the ACCC, which should be primarily responsible for competition and consumer issues and standards-setting. The OAIC should remain primarily responsible for privacy protection. ASIC, APRA, the RBA, and other sector-focussed regulators as applicable, should be consulted where necessary.

Assessment and designation of sectors

Potentially in some sectors or for some data sets, the benefit to customers of introducing the CDR would not outweigh the costs to data holders, or justify the risk to customers of sharing the data. The regulatory framework needs to include a process of assessment to identify sectors and data sets the CDR should apply to. This assessment would include regulatory impact analysis and privacy impact assessments, based on consultation with industry and the public. Where it is found that it is not currently suitable to implement the CDR in a sector, the assessment may be revisited in the future following technology or other changes.

The Government has announced that Open Banking will be the first sector of the CDR, based on assessment undertaken in the PC's Data Report. Judging by the submissions to this Review and consultations, that assessment has been confirmed, subject to an effective implementation.

In future, the ACCC should conduct sector assessments, in consultation with the OAIC, customers, industry, and the relevant sector regulators. For Open Banking, the ACCC may periodically need to consider whether the scope should be expanded through additional relevant data sets, or whether the implementation timetable needs to be adjusted.

The decision to apply the CDR to a sector may have significant budgetary implications and will need therefore to align with other Government priorities. As such, the Minister responsible for competition (i.e. the Treasurer) should hold the power to apply the CDR to a sector. Banking should be designated under regulation accompanying the amendments to the CCA.

Recommendation 2.3 – the banking Consumer Data Right

Banking should be designated as a sector to which the Consumer Data Right applies.

Rules that apply to designated sectors

To complement the principles-based amendments to the CCA, Rules would be required to specify what the CDR needs to achieve in designated sectors, including banking. The Rules could also set out guiding principles that could assist in the development of the Standards. As far as possible, the Rules should be non-prescriptive regarding technology in order to avoid creating barriers to entry or inhibiting technological innovation.

Who should be responsible for setting the Rules?

Under the regulatory partnership model described above, the ACCC would have primary responsibility for writing the Rules, in conjunction with the OAIC (which should have responsibility for ensuring the Rules' interaction with the Privacy Act), and in consultation with ASIC, APRA, RBA and other relevant regulators. Devolution of the rule-making power to the ACCC should maximise flexibility. In developing the Rules, the ACCC should consult publicly to ensure that the Rules reflect the needs of the community and of industry.

Providing the ACCC with the power to make rules will maximise flexibility and allow for greater consultation with participants. Requiring Ministerial consent to the Rules would provide a system of checks and balances and ensure they align with Government policy generally. Ministerial consent would also provide a check on the level of prescriptiveness of the Rules, and balance on the division between the responsibilities of the Rule-makers and the Standards-setter. The Minister for competition (the Treasurer) should retain power to make regulations, and the Rules should be disallowable by Parliament to ensure accountability within the democratic process.

What should be included in the Rules?

The Rules, in conjunction with the Privacy Act, need to address customer rights and competition, as well as the confidentiality aspects of Open Banking. As the APPs under the Privacy Act do not apply to non-personal information, it may be necessary to include confidentiality rules in the CDR for such information (which includes business information) that mirror some of the protections in the APPs.

While the Rules for Open Banking should be based on the needs of the banking sector, in writing the Rules, the ACCC should have regard to consistency between sectors. Appendix E provides example 'direction to transfer' Rules, and an outline of suggested topics to be covered by the Rules.

As the CDR is applied to other sectors, the Rules in new sectors would need to be consistent with the Rules for Open Banking, but may not be identical, owing to the differing circumstances and technological starting points of different sectors. One method of achieving this may be to have general CDR Rules, which are accompanied by, and can be overridden by, sector-specific Rules where a different approach is required. This would promote consistency and create transparency in areas of difference between sector Rules.

Interaction of the Rules and other relevant laws

Open Banking will need to align a variety of existing legal frameworks, including contract law, banking law, competition law, consumer protection laws, and privacy law. The Rules should be consistent with existing laws, though clarification, variation, or enhancement might be required. As canvassed in submissions,[23] the Rules may need to clarify how existing laws interact, intervene where existing law needs to be extended, or resolve a conflict with existing law. For example:

- where the Rules require greater specificity than the existing law or require an existing law to be extended for CDR purposes, the ACCC should be responsible for writing Rules in consultation with relevant regulators, for example the OAIC, and
- where a Rule conflicts with an existing law, the Rules should take precedence for the purpose of the CDR, so long as the ACCC has consulted with relevant regulators.

Some examples of where the Rules need to modify the effect of existing laws in relation to Open Banking are provided in Chapter 4.

Recommendation 2.4 – Rules written by the ACCC

The ACCC, in consultation with the OAIC, and other relevant regulators, should be responsible for determining Rules for Open Banking and the Consumer Data Right. The Rules should be written with regard to consistency between sectors.

Standards

As discussed above, the third layer of regulation will come in the form of Standards. Standards for Open Banking (and other sectors designated under the Consumer Data Right) are required to ensure efficient and simple implementation and compliance, interoperability between accredited parties within and across sectors, and promote competition.

Experience in the energy sector has shown that insufficiently specified standards for data sharing can result in sub-optimal outcomes.[24] In 2016, rules came into effect in the National Electricity Market allowing customers to direct that a data recipient can obtain their electricity consumption data from

23. See for example, the ANZ submission, which addresses the issue in some depth at pages 28-32.
24. Energy Consumers Australia, 2017, Electricity Meter Data Portability Discussion Paper. Available at http://energyconsumersaustralia.com.au/wp-content/uploads/Electricity-Meter-Data-Portability-Discussion-Paper.pdf

Distribution Network Service Providers. However, the rules did not address detailed processes related to providing data to customers and their representatives.

Currently third-party providers in the energy sector need to negotiate bilaterally on identity confirmation and data access processes with every distributor. Some providers have chosen to require customer consent evidenced by a paper signature.

As submitted by Yodlee, standards can help overcome challenges for smaller institutions:

> *Understanding the relative challenges for smaller financial institutions, the Government may opt to make certain accommodations for these entities. In the United Kingdom, for example, a regulatory-sponsored effort saw the creation of a standardised API [Application Programme Interface] by the nine largest British banks, which all players in the financial system will be permitted to use at no cost.*[25]

The Regional Australia Bank also submitted that standardisation could aid smaller institutions in overcoming the inefficiency of bilateral arrangements:

> *While larger FIs [Financial Institutions] may wish to establish and maintain a direct relationship with third parties such as FinTech companies, the use of an intermediary or aggregator should be explored as an aid to entry for smaller institutions… This approach would streamline access to multiple institutional datasets for any fintech developers through a single access point.*[26]

Relying on a process of bilateral negotiations would be unworkable in a broader CDR, while a paper-based signature consent mechanism does not facilitate a well-designed customer experience.

What should be included in the Standards?

The Standards should specify the way in which accredited parties connect and how they will meet the Rules. Chapter 5 discusses what should be included in the Standards in further detail. In principle, the Standards include:

- **Transfer standards** – to enable uniform transfer methods, processes, and practices.
- **Data standards** – specifications by which data are described and recorded to provide data integrity, accuracy and consistency, clarify ambiguous meanings, minimize redundant data, and document business processes.
- **Security standards** – techniques to protect the cyber environment of a user or organization. This environment includes users themselves, networks, devices, software, processes, information in storage, applications, services, and systems.

The Standards should be relatively stable (whilst being able to evolve) over time, and allow accredited parties to efficiently connect and transfer. A layered approach to the Standard should be adopted, meaning that core Standards would specify solutions required to ensure interoperability. Supplemental non-binding Standards would be permitted, enabling innovation at the pace of the

25. Yodlee submission, page 3.
26. Regional Australia Bank submission, page 1.

fastest innovator. Accredited parties should only adopt additional standards if they are interoperable with the core Standards and if arrangements exist to support this interoperability without individual accredited parties having to build services that translate each accredited parties' individual form of implementation.

Recommendation 2.5 – the Standards

The Standards should include transfer, data, and security standards. Allowing supplemental, non-binding, standards to develop (provided they do not interfere with interoperability) will encourage competitive standards-setting and innovation.

Who should be responsible for setting the Standards?

Standards need to be written with the close involvement of experts and industry to ensure that they are fit for purpose and able to evolve to the changing technological environment. As proposed in a number of submissions,[27] a special body given the responsibility of setting Standards would ensure that all participants and potential future participants have an opportunity to contribute. Given the need to coordinate disparate views, ensure a fair hearing for all potential participants and protect against barriers to entry, this Data Standards Body would be appointed by the Government. It would include potential accredited parties, customer representatives, and data transfer experts.

A Data Standards Body that is not captured by any one part of the sector, and incorporates technical expertise, would be more likely to ensure that the Standards remain fair and do not become an unreasonable barrier to entry. Experience in the process of standards-setting and of drawing upon the disparate experience and expertise of participants would be beneficial. Standards-setting is an evolutionary and iterative process, and Standards may be required for other sectors in the future under the CDR. As such, the Data Standards Body should have an ongoing role of reviewing Standards to ensure they continue to be fit for purpose.

The regulators, including relevant regulators such as ASIC, RBA and APRA, should have a role in the Data Standards Body as observers, while the ACCC should have the role of overseeing this body.

Recommendation 2.6 – a Data Standards Body

A Data Standards Body should be established to work with the Open Banking regulators to develop Standards. This body should incorporate expertise in the standards-setting process and data-sharing, as well as participant and customer experience.

In the initial transition period, the Government may consider the option of requesting a respected data expert like Data61[28] perform the functions of the Data Standards Body, with Standards Australia providing support in the standards-setting process. In the event that the Data Standards Body is

27. See for example the Australian Finance Industry Association submission, page 3 and the RBA submission, page 2.
28. Data61 is part of the CSIRO and is Australia's leading digital research network.

unable to produce Standards within a reasonable time, the ACCC should retain standards-making powers, in consultation with the OAIC, and the sector.

Interaction of the Rules and the Standards

The Rules should specify the need to adopt the core Standards and comply with them. Compliance with the Standards would evidence compliance with the obligations in the Rules and be enforceable by the regulator if necessary. The Standards should have the effect of a multilateral contract and be directly enforceable between accredited parties. Parties should not be able to contract out of the provisions of either the Rules or the Standards.[29]

Accreditation

Currently, banks run their own processes for approving entities before entering into data sharing arrangements. This is time consuming, costly and results in exclusive relationships that could inhibit competition. A standardised process would reduce the cost to potential data recipients, allowing them to provide their services to customers following a single accreditation process.

Accreditation would create a list of parties who are considered trustworthy, due to their compliance with a set of requirements. A customer's banking data is valuable information and its misuse can lead to damage or financial loss. Those who receive and hold data under Open Banking should therefore be required to safeguard that information.

The UK has decided to limit access only to accredited third parties known as 'whitelisted parties'. A bank would only comply with a customer's request to transfer their data to a third party if that party is 'whitelisted'. This limitation of access reduces risk and gives users greater confidence in sharing data. The EU's PSD2 also contains an accreditation process.[30]

Submissions to the Review indicated support for an accreditation process for data recipients, arguing that this would create greater customer confidence.[31] Many submissions also advocated for varying levels of accreditation to recognise the risks associated with different data sets. A graduated accreditation approach would address concerns regarding barriers to entry for small start-ups.

From the customer's perspective, an accreditation process is desirable. Accreditation would allow customers to determine with greater ease which data recipients meet the Standards and may, as a result, be considered trustworthy. An accreditation process should inspire confidence amongst customers to share their data with recipients that the customer has chosen to trust. An accreditation process would also provide some level of customer protection from malicious third parties.

The Review notes that, in conducting assessments for future CDR sectors, the ACCC and OAIC may conclude that a sector does not require accreditation. The assessment process should therefore

29. In the same way that financial market operating rules are often enforceable between parties.
30. The second Payment Services Directive (PSD2) allows customer directed retrieval of bank account data by accredited parties.
31. ANZ, ABA, Australian Payments Council, Australian Payments Network, CBA, Cuscal, COBA, FinTech Australia, Moneytree, NAB, RBA, Westpac, and Xero.

explicitly consider if a sector or data set is one where accreditation is required, and provide an assessment of the degree of accreditation required.

Who should be responsible for setting accreditation criteria?

FinTech Australia,[32] Westpac,[33] and ANZ[34] submitted that the regulators should be responsible for setting accreditation criteria. Factors that support this proposal include the importance of the accreditation process for the protection of customers, and the potential for this process to be misused in an anti-competitive manner.

Some submissions to the Review, notably that of the ABA,[35] proposed that an industry working group, or industry run utility, should be responsible for accreditation. After careful consideration, the Review does not support this option. An industry run utility may struggle to overcome the problem of coordinating diverse views, and to balance privacy and efficiency considerations due to perceptions of bias towards incumbent participants. The submissions show that there already exists a strong difference of opinion between participants in the banking sector as to the criteria for accreditation. There is a clear role for government in balancing these interests. In this context, an industry run utility would not be appropriate to accredit parties to a broader system. It would be preferable for the lead CDR regulator, the ACCC, to perform this function.

Recommendation 2.7 – accreditation

Only accredited parties should be able to receive Open Banking data. The ACCC should determine the criteria for, and method of, accreditation.

Accreditation criteria

The requirements to satisfy an accreditation process, as well as the manner in which such a process can be satisfied, are important features of the implementation of Open Banking. There is a balance to be struck between the safeguards needed to promote confidence and a sustainable Open Banking system, and avoiding creation of unnecessary barriers to entry and innovation.

Submissions to the Review put forward a number of relevant considerations including, the ability to meet security standards, publication of internal dispute resolution processes (IDR), membership of an external dispute resolution (EDR) body, and mandatory breach notification. Further, in many submissions the issue of having adequate insurance to compensate customers for any loss was an important requirement for data recipients to be able to participate in Open Banking.[36]

32. FinTech Australia submission, page 23.
33. Westpac submission, page 12.
34. ANZ submission, page 33.
35. ABA submission, page 5.
36. ABA, CBA, Envestnet Yodlee, FinTech Australia, Moneytree, NAB, and Westpac.

Some submissions proposed accreditation based on 'use cases'.[37] The Review does not recommend accreditation based on the proposed use for the data. Customers should be free to choose their own uses and seek value outside of that currently considered by industry or regulators. As discussed in the PC's Data Report,[38] there are no ownership rights to data in Australian law, but there are various access and use rights. For a transfer right such as the CDR to be effective in encouraging competition and innovation, customers must be able to choose the purpose of that transfer, without interference from regulators or data holders. Many future uses of data available to customers through Open Banking and the CDR have not yet been conceived, may rely upon the creation of future technologies, or may become apparent as new sectors are added. Limiting accreditation to use cases that exist at this moment in time would limit these future innovations.

International models

The process for accreditation adopted in offshore jurisdictions does provide some further indication of issues that might be considered for Australia. For example, the EU's PSD2 also provides guidance on an accreditation process and specifies that an application to be authorised as an account information services provider should include for example:

- the description of the governance arrangements and internal control mechanisms
- the description of procedures to deal with security incidents
- the description of the process in place to file, monitor, tract and restrict access to sensitive payment data
- a security policy document, and
- the identity of directors and persons responsible for management.

In the UK, to be accredited, third parties need to:

- provide security policies and procedures, including a risk assessment in relation to payment services,[39] and describe security controls and mitigation measures
- demonstrate that they have effective processes to monitor and handle incidents and security-related customer complaints
- explain how they will deal with significant continuity disruptions, such as the failure of key systems, the loss of key data, or lack of access to premises, and
- demonstrate that they have an effective process to file, monitor, track, and restrict access to sensitive payment data such as data classification, access management, and monitoring tools.

A tiered accreditation model

Given that technology changes rapidly, as do potential uses and risks associated with data, accreditation should entail more than a one-off process. However, accreditation should not require that unnecessarily intensive, or expensive, official certifications be obtained. To balance these considerations, and allow for adaptability across sectors, the regulators should consider a tiered (or, graduated) accreditation model. Under a tiered accreditation model, parties would be accredited to

37. See for example ANZ submission, page 40; CBA submission, page 4; and, NAB submission, pages 7,9.
38. PC Data Report, page 196.
39. Note that the UK Open Banking model includes the ability for accredited third parties to initiate payments on the customer's behalf.

receive and hold data, based on the potential harm that the relevant data set and that party pose to customers, and to the Open Banking system.

Tiered accreditation would allow for a more flexible application of the burden of accreditation. Assigning sectors and data sets to a tier also avoids the inefficiency of accrediting parties to each additional sector as it is added to the CDR.

Under a tiered accreditation model, requirements would reflect the risk of the data held by the accredited party and the parties' proposed risk management systems. Both data sets and parties would undergo a risk assessment and be assigned to an accreditation tier:

- data sets would be assessed as being a higher or lower level risk[40] based on the harm that may arise if there were to be unauthorised access to the data.[41]
- parties would be accredited to receive[42] either higher risk or lower risk data sets:
  - parties who are accredited to receive lower risk data sets would not be able to receive higher risk data. In such a model, lower risk accreditation could be more like a registration process.
  - parties who are accredited to receive higher risk data would be able to receive both higher and lower risk data sets.[43] In considering whether to accredit a party to a higher tier, the ACCC should ensure it is satisfied that the systems and resources in place for controlling or mitigating risks, and the risk management framework, are appropriate to the party. For many higher tier parties, the accreditation requirement may be an annual declaration of the sufficiency of their systems, resources, and risk management frameworks based on self-assessment.[44]
  - lower tier accredited parties could work with higher risk data sets behind the data security firewalls of higher tier accredited parties if the parties choose to establish arrangements allowing this.

Though the ACCC should be responsible for ensuring the process and criteria by which accreditation occurs, it does not need to undertake accreditations itself. Accreditation could be based on reviews conducted by qualified third parties.

40. There could be a more precise manner of designating the risk associated with data sets and parties. However, the designation of higher and lower risks serves the explanatory purpose of this Report.
41. In considering this harm, the ACCC should consider factors including whether the information is sensitive information under privacy law, its release could result in damage to personal health or reputation, or would be commercially damaging to the customer were it made publicly available. Systemic risk considerations are also important. The Review would expect that sensitive information would be a higher risk data set, while the regulators may consider summary data such as account balances to be lower risk data sets. For a guide to what may be considered sensitive information see section 6 of the *Privacy Act 1988* and OAIC, 2015, APP Guidelines Chapter B: Key concepts. Available at: https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts#sensitive-information
42. In creating the tiered accreditation model, regard should also be had to whether participants are receiving but not holding data, as part of assessing risks.
43. This is an important foundation in ensuring that there is a single cross-sector CDR regime.
44. See for example, APRA Prudential Standard CPS 220 Risk Management, Attachment A – Risk Management Declaration.

The Review considers that the ACCC should further consult with relevant sectors to determine accreditation criteria as part of the Rule setting process, and ensure that accreditation is based on objectively determined standards. Criteria that may influence a finding that a party has sufficient systems and resources in place to control and mitigate material risks include whether the party:

- is compliant with the privacy and confidentiality safeguards which are described in Chapter 4, including the provision, and publication, of IDR and EDR processes
- can provide evidence of risk management processes and measures,[45] including in regard to their outsourcing arrangements
- can demonstrate processes to test the effectiveness of customer consent, including understanding of what has been consented to
- has the technical capabilities to meet the Standards, and
- has a history of data breach or misuse, or of disregard for the law.

Interaction with existing licensing regimes

In setting the criteria for accreditation, the ACCC and OAIC should have regard to existing licensing regimes within sectors. The regulators should consider whether licensing regimes that require compliance with the Privacy Act and specify security standards meet the accreditation criteria for Open Banking and, if so, the ACCC can recognise existing licenses. For Open Banking, accredited parties who are Authorised Deposit-taking Institutions (ADIs) should simply require registration to participate.

The Review considers that determination of accreditation standards should be risk-based. For example, the current standards applicable to banks take into account that banks hold more than data of customers, they hold their money as well. In most cases, payment of money is a higher order risk than the transfer of records of those payments. As such, in setting the requirements for higher risk accreditation, the ACCC should not seek to apply the same accreditation standard as required for authorisation as an ADI.

Allowing foreign accredited parties into the Open Banking system

Several other jurisdictions are currently in the process of implementing open data regimes. As noted above, the UK's regime will have a 'whitelist' of approved parties and utilises a definition of 'competent authority' that could allow whitelisting (accreditation) of approved parties from other EU countries.[46]

While providing mutual recognition of accredited parties (known as passporting) may amplify the benefits that Open Banking is seeking to achieve, ensuring that customers in Australia have the trust and confidence to engage in Open Banking is a priority for the Review. All parties receiving customer data under Open Banking should therefore be subject to Australian laws (i.e. laws requiring that information be kept confidential) and be accountable and able to meet any potential liability for loss suffered.

45. When a mature insurance market exists, this may include level of insurance coverage.
46. Open Banking Ltd, 2017, 'Glossary'. Available at https://www.openbanking.org.uk/about-us/glossary/

The ACCC should consider what would be needed to passport accredited entities from other jurisdictions into Australia's Open Banking system once the regimes in both jurisdictions are established.

Conduct related to accreditation

Adherence to, and respect for, the accreditation system is fundamental to the sustainability of the CDR regime. It should be a reportable breach of the Rules if a data recipient requests a data set that is rated to a higher risk level than they are accredited to receive, or if a data holder transfers a data set that is rated to a higher risk level than the requesting data recipient is accredited to receive. The remedies for this should include deletion of collected data, blocking of the website or app, and civil penalties. Where an act has been undertaken for a dishonest or fraudulent purpose, criminal penalties should apply.

Accredited parties in the system will rely on their accreditation to give them access to a customer's information at the customer's direction.[47] Accordingly, any unilateral action to refuse to provide an accredited party with data sets they are accredited to receive should be a serious competition issue. Any refusal action by data holders to stop the transfer of data (other than at the customer's request) should be a last resort, and only be undertaken in circumstances where waiting for action by the regulator is considered likely on reasonable grounds to result in a data breach. Such unilateral refusal action would itself be potentially a serious competition and systemic issue, and as such, should be mandatorily reportable by both parties.

The ACCC and OAIC should convene within a business day of an action to consider the evidence available to the accredited party who took the unilateral refusal action. An unreasonable refusal action should be a breach of the Rules. This breach of the Rules should be actionable by the data recipient, the data provider's customers, and regulators. The data recipient's access to the data should be restored immediately.

Regulators' decisions on accreditation or de-accreditation should be reviewable by the Administrative Appeals Tribunal.

Recommendation 2.8 – the accreditation criteria

Accreditation criteria should not create an unnecessary barrier to entry by imposing prohibitive costs or otherwise discouraging parties from participating in Open Banking. Using a tiered risk-based accreditation model and having regard to existing licensing regimes should minimise costs for many participants. Accreditation decisions should be reviewable by the Administrative Appeals Tribunal.

47. For example, it will be important that data holders do not use additional requirements (such as requirements for specific data holder-approved use cases or additional verification steps, including wet ink signatures) which go beyond the Rules, Standards and accreditation regime to limit a customer's right to share information with accredited parties.

Other supporting infrastructure

Other than accreditation, two further pieces of supporting infrastructure or services are necessary to ensure the effective operation of Open Banking. These are the provision of an address book and developer resources such as technology sandboxes.

Address book

Given that banking is a sector that requires accreditation, the regulatory framework needs to incorporate an address book for participants and customers to be able to know whether a party is accredited and the tier of accreditation held. Given the ACCC will have responsibility for accreditation it should also have responsibility for maintaining the address book.

If the ACCC decides to arrange for other regulators or private parties to provide accreditation services, the decisions of these parties need to be reflected in this address book. To reflect the liability framework discussed in Chapter 4, the address book needs to be live, robust, and ideally decentralised. The address book also needs to be secure, transparent, and include a method of tracing all changes made.

Many CDR participants will participate across sectors. Only authorised accreditors should have the authority to alter the address book. The ACCC might want to consider the use of a permissioned distributed ledger technology for the address book.[48]

Recommendation 2.9 – responsibility for the address book

The ACCC should have responsibility for ensuring there is a public address book showing who is accredited.

Developer resources

Developer resources such as technology sandboxes would promote interoperability and competition in Open Banking. Though the regulatory framework includes a process of standards-setting, some technical and interoperability issues are likely to continue to arise. To overcome these issues developer resources including technology sandboxes should be provided. Technology sandboxes are testing environments that exist in a virtual space in which new or untested software or coding can be

48. Distributed ledger technology such as blockchain offers a number of benefits when used for an accreditation address book. These benefits include "An industry's shared ledger may have a limited number of fixed validators who are trusted to maintain the ledger, which can offer significant benefits. Participants may be permissioned by the rules to distribute and receive different data to others in the network… Centralised or institutionalised systems with a 'hub and spokes' design, pose the risk of high cost and a single point of failure. If that point of failure is a systemically important institution that may have implications for the stability of the wider financial system. Distributed ledgers open the possibility of avoiding this through replication…. A regulator may desire certain competencies or resources of participants that are allowed to receive or distribute data when they present required authentication and evidence of authority." See Kingsford-Smith, D, 2017, "Distributed Ledger Technology and Blockchain in Financial Regulation", UNSW Centre for Law, Markets and Regulation, Working Paper for Regulators' Forum 25 October 2017, pages 3- 4.

run securely. The experience of Macquarie Bank providing a technology sandbox shows the incentives to create these resources.[49]

The Review considers that the banking sector should be given a reasonable period to develop these resources. Industry developed resources would need to be consistent with the Standards, and subject to oversight to ensure that they are not incorporating barriers to entry. Processes should be in place to ensure that developer resources do exist if industry fails to create them. Subject to further decisions of Government regarding the design of the Data Standards Body, either the ACCC or the Data Standards Body could reasonably be responsible for ensuring the provision of developer resources.

Compliance

Existing experience with data transfer demonstrates that issues may occur which would result in losses to customers or other participants.

The Review has identified four broad categories of issues that may arise within the CDR regulatory framework. These are:

- individual customers' complaints regarding privacy
- business customers' complaints regarding confidentiality
- customers' complaints regarding competition, and
- accredited parties' complaints regarding the conduct of other accredited parties (these issues are likely to be competition based, but may also arise from the breach of individuals rights).

Under the existing privacy and competition regimes, significant gaps would exist for business confidentiality issues and competition issues related to the CDR. Without a means to address these issues, accredited parties cannot be assured that potential losses will be resolved or that the system as a whole will remain effective into the future.

Customer complaints

Complaint handling

At the complaint handling level, practical and accessible IDR and EDR methods should be required. As discussed in Chapter 4, within the banking sector, and more broadly in other sectors, a number of EDR schemes already exist and should be utilised to resolve complaints.

To avoid creating a dispute resolution framework that would result in overlapping jurisdictions and multiple contact points for customers, complaint handling needs to be primarily addressed by a single point of entry to the complaint handling body. As proposed in the PC's Data Report, there should be 'no wrong door' for customers. It is more efficient for the regulators to accept and then

49. See for example, Eyers, J, 2017, 'Macquarie trumps big four with open banking platform'. Available at http://www.afr.com/business/banking-and-finance/macquarie-trumps-big-four-with-new-open-banking-platform-20170914-gyhbxy

direct all complaints through a Consumer Data Contact Point (a virtual point of contact, such as a single telephone number and webpage, which connects complainants to complaint handlers), than to expect customers to determine which regulator is the best in the circumstances. Customers would then be able to access the one point of contact for both privacy and competition related complaints.

As discussed in detail in Chapter 4, for individuals and some small businesses,[50] privacy, confidentiality and competition issues are likely to be inextricably linked. An option would be to create a new Consumer Data Agency to hear individual and small business (up to a turnover of $3 million per annum) complaints. However, this option would involve significant, and costly, duplication of existing functions. The OAIC currently handles complaints regarding private information, including the private information of small business owners in relation to their business activities. However, the OAIC does not handle complaints regarding the confidentiality of small business information, though this may exist within the same data set. Given that, from an individual trust perspective, the more serious of privacy, confidentiality, and competition issues, are likely to be privacy issues, the Government may consider it appropriate for the OAIC to fill the role of this complaint handling body.

Right to remedy

In the event that disputes regarding alleged breaches of the CDR cannot be resolved through IDR or EDR, the amendments to the CCA should give customers standing to seek remedy through the courts.

Recommendation 2.10 – customer complaints and remedies

Open Banking should have internal and external dispute resolution processes to resolve customer complaints. Amendments to the *Competition and Consumer Act 2010* should create powers to address complaints (to the extent these do not already exist) and give customers standing to seek remedy for breaches of their rights. There should be a single consumer data contact point - there should be 'no wrong door' for customers. The OAIC should retain enforcement powers in relation to privacy and could also be given enforcement powers of confidentiality for businesses.

Accredited parties' complaints on the conduct of other accredited parties

The customer may not consider some breaches worth pursuing. For example, if a data holder does not transfer a complete data set (as requested by the customer) to an accredited recipient, this refusal to transfer would be a breach of the customer's right to transfer. The loss to the customer may simply be that they do not obtain the service they were hoping to from the recipient (for some customers, this may not be particularly costly). However, for recipients who have experienced refusals, these refusals may be costly as they could significantly affect the recipient's business model.

50. OAIC, 2017, 'What is personal information?' Available at https://www.oaic.gov.au/agencies-and-organisations/guides/what-is-personal-information

There are also circumstances where businesses may act in an uncompetitive manner that does not affect individual customers, for example, by refusing to provide developer resources. Confidence in Open Banking includes trust that the system will function in a stable manner. Significant uncompetitive activity of this kind has the potential to affect the system as a whole. As the Standards would be a contract between accredited parties, parties would have a right to take action for breach in these circumstances. Accredited parties should commit to resolving these disputes through EDR where possible.

There is a public interest in service providers reporting these categories of breaches to the ACCC and in giving the ACCC enforcement powers regarding these breaches.

Recommendation 2.11 – remedies for accredited parties

The Rules should create a right for accredited parties to seek remedy for breaches of the Consumer Data Right. There should also be breach-reporting obligations to the ACCC.

Enforcement

To regulate the CDR system effectively, the ACCC should have broad research and investigative powers.[51] To enable the ACCC's enforcement function, the OAIC and any other complaints handling body should report all CDR complaints to the ACCC. The OAIC should continue to analyse complaints it receives for systemic privacy enforcement purposes and may gain enforcement powers related to confidentiality rights under Open Banking.

The regulators should be provided a range of remedies to enforce the CDR, including:

- directions powers for the deletion of data[52]
- directions powers for audits and reviews
- directions powers to otherwise enforce compliance
- movement to a lower accreditation tier, temporary suspensions, and permanent bans from the CDR system
- compensation orders
- civil penalties, including an infringement notice regime, and
- criminal penalties for serious breaches.

51. Systemic competition issues may include repeated instances of anti-competitive conduct, or serious singular instances. The ACCC's compliance and enforcement policy is available at https://www.accc.gov.au/about-us/australian-competition-consumer-commission/compliance-enforcement-policy
52. As a punishment or remedy for a breach by an accredited party, as opposed to a choice generally available to customers.

The compliance structure would be as summarised in Table 2.1 below.

Table 2.1: Proposed compliance structure

	Individual privacy	Business confidentiality	Customer competition	Accredited party competition
Individually enforceable rights	Individuals have right to remedy regarding use of the CDR	Businesses able to enforce rights under CCA	Customers able to enforce rights under CCA	Businesses able to enforce rights under CCA
Complaint Handling	OAIC	OAIC	OAIC	ACCC
Enforcement of systemic issues	OAIC	OAIC	ACCC	ACCC

Extraterritorial effect

Both the Privacy Act and the CCA contain provisions that extend the operation of the Acts to an act done, or practice engaged in, outside Australia and the external territories.[53] A key case in interpreting the definitions of 'conducting business in Australia' and 'engaging in conduct outside Australia' is *Australian Competition and Consumer Commission v Valve Corporation* (No 3) [2016] FCA 196. The reach of Open Banking and the CDR should align with these existing laws. The existing provisions of the CCA and Privacy Act should therefore have extra-territorial effect to capture Open Banking conduct occurring in Australia by accredited parties, or parties purporting to be accredited.

Applying the *existing* extraterritoriality tests, Open Banking would apply to data related to a good or service provided in, or to conduct occurring in, Australia; or to data related to a good or service provided by a business or individual that is located in Australia.

This may, however, be limited by the terms of the data designation.

53. See section 5B of the Privacy Act and section 5 of the CCA.

Chapter 3: The scope of Open Banking

This chapter sets out recommendations about which participants and data sets should be designated as in scope for the banking sector, on the basis that it becomes a designated sector under the broader Consumer Data Right (CDR) discussed in the previous Chapter.

In setting these parameters the Review is not attempting to identify the data sets that will be of the highest potential value to customers. Customers themselves, in conjunction with providers of data-related products and services, are best placed to determine that. Moreover, innovations in technology and financial services, together with changing customer preferences, will mean that the value of particular data sets change over time as Australia's emerging data industry matures.

Although the Review has been asked to set the design parameters for sharing *banking* data, 'banking' is not the sole prism through which that design should be approached. The CDR will eventually apply across a number of sectors and the design of Open Banking should be approached with this in mind.

What types of data should be shared?

It is clear from submissions and consultations that Open Banking means different things to various parties. To clarify and define the scope of Open Banking, the Review has found it convenient to start by dividing the data potentially in scope into categories covering a spectrum of connectivity to the customer. From most closely-connected to least closely-connected, these categories are:

- **Customer-provided data** — information provided directly by customers to their banking institution.
  - examples include: a customer's personal address and contact details; information on their financial situation provided when opening an account, or applying for a loan; and information that has been provided for the purpose of making payments, such as payee lists.
- **Transaction data** — data that is generated as a result of transactions made on a customer's account or service.
  - examples include: records of deposits, withdrawals, transfers and other transactions undertaken by a customer (such as direct transactions with merchants); account balances; interest earned or charged; and other fees and charges incurred by the customer.
- **Value-added customer data** — data that results from effort by a data holder to gain insights about a customer.
  - examples include: income/assets checks; customer identity verification checks; credit reporting data; credit scores; data on an individual customer that has been aggregated across the customer's accounts and standardised, cleansed or reformatted to make it more usable.

- **Aggregated data sets** — created when banks use multiple customers' data to produce de-identified, collective or averaged data across customer groups or subsets.
  - examples include: average account balances by postcode or income quintile, or average size of small business overdrafts by industry segment.

The paragraphs below examine these categories in turn.

Customer-provided data

Personal details and information on their financial situation that a customer has provided to a bank clearly 'belong' to the customer. It can be provided to anyone they chose, without any argument being raised that it did not belong to them to do so, or did not belong to them exclusively. In principle, customers should have the right to instruct that it be given to them, or shared with data recipients they choose, in a form that facilitates its transfer and use.

Although some of that information may have originally been provided to the bank in paper form, a copy of it will usually have been converted by the bank for digital capture and electronic storage. By itself, that conversion should not have altered the information. Similarly, while the customer may have provided the data over a considerable time period and the bank may have developed a central repository through the customer's account record, the simple collection of the data into a convenient record should not have materially altered it.

The time and effort involved in providing these details to a competing provider is a significant factor behind observed low rates of switching in the Australian banking market.[54] If a customer applying for a new account could simply instruct their current provider to share their personal details with a new provider, relieving them of the need to go through that part of the application process again, the 'hassle factor' associated with switching between providers would be significantly reduced.[55]

An exception to the above principle relates to information provided by the customer to support identity verification. A number of submissions to the Review argued that making data used to verify customer identity available in a packaged electronic form could significantly raise the risks of identity theft. A general view emerged in consultations that, rather than providing the identity data itself, it might be better for banks to provide only the *outcomes* of identity verification assessments. This would minimise the fraud risk while removing the hassle factor described above. However, this approach could only work if the data recipient could rely on that verification for the purposes of the Anti-Money Laundering (AML) laws, as if it had been performed by the data recipient.

A statutory review of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) tabled in Parliament in April 2016 recognised that the ability to rely on the

54. In 2016 credit bureau Experian surveyed 1,000 Australian banking customers to identify their 'pain points'. More than 40 per cent of respondents reported paperwork and lengthy application processes as a major pain point for Australians applying for a new credit card, loan or mortgage (RFI Group, 2017). Available at: https://www.rfigroup.com/australian-banking-and-finance/news/open-banking-lessons-australia%E2%80%99s-credit-industry
55. Other impediments to switching include: having to rearrange recurring payments and direct debits when switching to a new account; the inability to port banking account numbers between different providers; and behavioural biases, such as customer inertia.

identification of another party would be an important measure that could deliver greater efficiencies and significant regulatory relief for reporting entities under the AML/CTF regime in contrast to the model currently available.[56] That review recommended an enhanced model that should generally permit reporting entities to rely on identification procedures conducted by a third party. Since, in supplying the data to a third party under Open Banking, the original data holder is implicitly warranting that the data belongs to the customer directing that it be supplied, allowing formal reliance on that assurance would seem to be a small step. This approach and its consequences are discussed further under *Value-added customer data*.

Recommendation 3.1 – customer-provided data

At a customer's direction, data holders should be obliged to share all information that has been provided to them by the customer (or a former customer).

However:

- The obligation should only apply where the data holder keeps that information in a digital form.
- The obligation should not apply to information supporting an identity verification assessment. Data holders should only be obliged to share that information with the customer directly, not a data recipient.

Transaction data

The second category of data examined is the data generated as a direct result of a customer's interactions with their bank. These may be the records of deposits or withdrawals, interest earned or incurred, or other fees and charges. These records are already displayed to the customer via internet or mobile banking, or via paper-based account statements.

Some submissions have suggested that, although this data is *about* the customer, it was created by the data holder and is therefore effectively *not* the customer's data. Other submissions have clearly assumed that such data falls within the scope of data that customers should be able to share with other parties. The Review considers that customers have legitimate interests in the use of such data because they were essential to its creation. Without their involvement, by initiating a transaction or making repayments on an outstanding loan, the data would not have been generated. That is not to say, however, that such data belongs exclusively to the customer. Banks were also a party to its creation and both parties should be entitled to use the information subject to existing privacy and other restrictions.

A multitude of potential uses can be imagined for transaction data. A customer could share receipt and payment patterns or credit card transactions with a comparison services provider to obtain budgeting advice or a recommendation on the best credit card for them. Giving a customer the

56. The findings of the review are set out in the *Report on the Statutory Review of the Anti-Money Laundering and Counter Terrorism Financing Act 2006 and Associated Rules and Regulations.* The Report is available at: https://www.ag.gov.au/Consultations/Pages/StatReviewAntiMoneyLaunderingCounterTerrorismFinActCth2006.aspx

ability to easily share their transaction account data with a competing provider would also significantly ease the process of applying for a new product, such as a mortgage. Instead of having to provide scanned copies (or screenshots) of their past account statements, a customer could simply instruct their current provider to transfer a copy of that data to the potential new provider.

How much historical data should be provided?

The Review considers that it would be an excessive burden for a data holder to be obliged to share transaction data on a customers' instruction for an open-ended period. A pragmatic approach could be that data holders only be obliged to transfer data for the same period they are required to hold it for under existing regulatory obligations. Currently, the AML rules require that an entity must retain records (or a copy or extract) for seven years after making a transaction record that relates to providing a designated service to a customer. The obligation to retain transaction records applies to closed accounts, but only for seven years.[57]

In the initial stages of Open Banking, a requirement to provide seven-years of transaction data could impose significant costs on data holders as it is longer than they currently make data available to their customers via internet or mobile banking. Some costs may therefore arise as that data has not been stored in an electronic form. On the other hand, feedback from potential data recipients indicates that in many cases, receiving data that relates to an extended period would be relevant and valuable.

In a mature system, several years from now, it is likely that data will have been stored electronically for the full period that the banks are required to keep records. However, the Review recognises that transitional arrangements may be required during the initial phase of Open Banking. Transitional issues are discussed in Chapter 6.

Data on which products should be in scope?

A number of submissions to the Review argued that specific categories of data (including summarised transaction data) should be progressively made subject to the obligations based on whether there are clear and demonstrable applications for such data (the so-called 'use cases'). However, this approach would not be consistent with the Review's general position that customers themselves are best placed to determine the data types that are of the highest value to them. In addition to the range of possible uses currently, evolving customer preferences and future innovations in financial services will lead to the development of new uses for this data over time. Limiting the scope of Open Banking to specific uses would unnecessarily constrain that future innovation.

The Review has therefore concluded that data should be made available on those products relating to the conduct of banking business — as defined in the *Banking Act 1959* (Banking Act) — but only for those products that are widely available to the general public.[58] Specifically, the Banking Act defines banking business as being carried on by a corporation to which paragraph 51(xx) of the Constitution applies and that consists, to any extent, of: taking money on deposit and making

57. See Part 10, Division 2 of the AML/CTF Act.
58. There are also many banking products especially designed for individual customers, who are usually large business or wealthy individuals. The Review did not consider that there would be sufficient advantage bringing those into Open Banking.

advances of money; or other financial activities prescribed by the regulations (relates to purchased payment facilities).[59]

For certainty, the Review proposes the following products be expressly covered:

Table 3.1: Proposed list of banking products

Deposit products	Lending products
Savings accounts	Mortgages
Call accounts	Business finance
Term deposits	Personal loans
Current accounts	Lines of credit (personal)
Cheque accounts	Lines of credit (business)
Debit card accounts	Overdrafts (personal)
Transactions accounts	Overdrafts (business)
Personal basic account	Consumer leases
GST and tax accounts	Credit and charge cards (personal)
Cash management accounts	Credit and charge cards (business)
Farm management deposits	Asset finance (and leases)
Pensioner deeming accounts	
Mortgage offset accounts	
Trust accounts	
Retirement savings accounts	
Foreign currency accounts	

Recommendation 3.2 – transaction data

At a customer's (or former customer's) direction, data holders should be obliged to share all transaction data in a form that facilitates its transfer and use.

The obligation should apply for the period that data holders are otherwise required to retain records under existing regulations. Table 3.1 describes the list of accounts and other products to which this obligation should apply.

Value-added customer data

The third category is 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. 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, or interfere with existing commercial arrangements. At the very least it would represent a transfer of value from the data holder to the customer.

59. See Section 5 of the Banking Act.

Some submissions have argued that including such data in the scope of Open Banking would reduce incentives to invest in data analysis and transformation.[60] Data holders invest heavily in analysis to give themselves an edge over their competitors and create new business opportunities. If Open Banking (and broader access to data reforms) is to support the creation of an innovative Australian data industry, retaining incentives to make those investments will be important. Imposing an obligation that data holders share such information with other parties (including their direct competitors), if instructed to do so by a customer, could confer an unfair advantage on their competitors. This could make data holders less likely to make those investments, although the Review notes that the PC Data Report expressed some scepticism that a broad application of the CDR would discourage data holders from investing in data analysis.[61]

Recommendation 3.3 – value-added customer data

Subject to Recommendation 3.4, data that results from material enhancement by the application of insights, analysis or transformation by the data holder should not be included in the scope of Open Banking.

Again, however, there can be exceptions to, or qualifications of, this broad principle. Identity verification processes in financial services (often referred to as 'know-your-customer' or 'KYC' data) are slow and cumbersome and involve significant duplication.[62] As discussed above, granting customers the right to instruct their bank to share *the result of* an identity verification assessment performed on them could improve efficiencies in the system. A bank could simply affirm whether the customer is who they say they are without sharing the original data or data on the process by which that conclusion was reached. This approach would make it easier for customers to switch between providers by simplifying the process of sending copies of their personal documents and increase the efficiency with which competing providers are able to secure and on-board new customers. It would also enhance customer privacy and security, as obtaining access to the supporting documents provided by an individual as part of an identity verification is one of the most common methods of identity theft. Reducing the frequency with which customers are required to transfer such documentation will help to reduce that risk.

As a result, there are strong arguments in favour of creating an obligation to share the *result* of that verification or KYC process and *not* the supporting documentation provided by the customer. However, concerns about who bears the liability for reliance on the identity verification are currently hampering that approach.

60. See, for example, submission from Xero, page 2. See also submissions from ANZ and the Business Council of Australia to the PC Data Report.
61. See PC Data Report, page 201.
62. The practical application of identity verification in relation to individual customers and corporate entity customers can be complex and costly. For example identity documentation and credentials are required to be provided (physically or digitally) by the customer to each and every regulated business from which a service is provided. Chapter 5 of the Statutory Review of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, Rules and Regulations tabled in Parliament on 29 April 2016 contained detailed discussion arising from stakeholder submissions in relation to KYC and customer due diligence. The conclusions and resulting recommendations highlighted the need for legislation and associated rules where possible to be simplified.

The AML laws impose obligations on a reporting entity to apply a risk-based process to verify the identity of a potential customer applying for a product or service.[63] The current interpretation of the reliance provisions by most providers is that they are too narrow in their current form and an entity cannot rely on the identity verification performed by another, although the laws do not specifically preclude this. The Review understands that AUSTRAC and the Attorney-General's Department are currently consulting with industry on a proposed legislative model to allow a recipient to rely on another's identity verification, and encourages that work to be completed as quickly as possible.

Recommendation 3.4 – identity verification assessments

If directed by the customer to do so, data holders should be obliged to share the outcome of an identity verification assessment performed on the customer, provided the anti-money laundering laws are amended to allow data recipients to rely on that outcome.

Aggregated data sets

The final category of data is that created when banks use multiple customers' data to produce de-identified, aggregated or averaged data across customer groups or subsets. There are potentially thousands of sets of collective banking data that would be of value to competitors and product innovators, including various permutations of average balances and spending patterns across customer groups and geographic locations. In most cases that value will have been created by the effort of the bank. If this aggregated data was included in the scope of Open Banking, value created by the bank would effectively be transferred to the customer or, more likely, a competitor. In these circumstances it would seem fair if charging was allowed, or — if the Government compelled transfer without charge — compensation was paid.

Fortunately, if transaction data is within the scope of Open Banking, it will not be necessary to include aggregated data in order to allow others to unlock its value. As competitors acquire transaction data at the direction of customers, they should be able to replicate the aggregations (at least to some degree) over time. For this reason, the Review has concluded that aggregated data need not be included in Open Banking, at least in its initial phase. However, that question should be revisited after the broader CDR becomes operational.

The Review also notes that public sector agencies currently provide a range of aggregated data sets. Regulators are bound by requirements to balance the public benefits of disclosure of data against any possible detriment to the commercial interests that the disclosure may cause. The PC Data Report argued that more explicit regulator mandates for increasing competition could help to

63. The customer identification procedures required of reporting entities are set out in Part B of the Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1) (the AML/CTF Rules). The customer identification procedures in the AML/CTF Act supersede identification procedures set out in the *Financial Transaction Reports Act 1988* (Financial Transaction Reports Act). The Financial Transaction Reports Act provided prescriptive rules, including the '100 point' identity verification test under which identifying information from various sources is worth a certain number of points. By comparison, the AML/CTF procedures are described as 'risk-based', leaving each institution to make an assessment of the information it needs to gather from its customers.

encourage the publication of more data by regulators. Recently, the NSW Government has chosen to share its data via a secure platform provided by Data Republic.[64]

Recommendation 3.5 – aggregated data

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

Product data

Banks hold a range of data on the features of products they offer to customers generally (referred to as *retail* products). For special customers, they also offer bespoke or individually designed products. Retail product information is highly relevant to customers when deciding between available financial products. For that reason banks and other financial services providers are currently bound by legislation to disclose information about those products, including details on their price, fees and charges.[65] However, the way that information is currently presented and the high degree of variability between competing products makes it difficult for customers to compare available product offerings.

As with categories of customer-connected data there would be significant value in making retail product data easily available, in a form that facilitates its digital use. Some submissions have pointed out the difficulties involved in translating some of this information into a digital form, particularly information that is more qualitative in nature. Nevertheless, technology innovators have pointed out that, if given the basic information, they can manage the challenges of comparing terms that are subject to interpretation.

Recommendation 3.6 – product data

Where banks are under existing obligations to publicly disclose information on their products and services — such as information on their price, fees and other charges — that information should be made publicly available under Open Banking.

64. See: https://www.cmo.com.au/article/628952/nsw-government-picks-data-republic-launch-data-sharing-platform/
65. Most disclosure obligations on banking products and services providers are imposed by the *Corporations Act 2001* and the *National Consumer Credit Protection Act 2009*.

Who should be able to direct data be shared?

The object of Open Banking is fundamentally about reducing information asymmetries — giving customers better access to the information they need to enable them to make better decisions and to seek out products that better suit their circumstances. Open Banking should therefore be available to those customer groups where information asymmetries are most significant.

Individuals

A number of recent reviews and inquiries[66] have found significant scope to improve individual consumer outcomes in a range of banking products and services. Reasons highlighted include: high market concentration (and therefore a lack of competition); widespread cross-selling of products and services; product complexity; consumer inertia and other behavioural biases. Open Banking could help to overcome many of those factors. Open Banking should, therefore, at least apply to individual customers, which, for practical reasons, means individuals who hold an Australian account.

Small businesses

The PC Data Report proposed that the broader CDR apply to small businesses, and a range of other evidence suggests that information asymmetries are particularly acute for small businesses. For example, the Interim Report of the Financial System Inquiry found that:

> *Information asymmetries are the most significant structural factor contributing to the higher cost and lower availability of credit for small-to-medium sized enterprises (SMEs) and can be a barrier to competition in SME lending.*[67]

Smaller businesses typically have less documentation and shorter financial histories, so it is generally harder and more costly for competing providers to acquire the required information to make accurate assessments of potential small business customers. A bank that has an established relationship with a small business is at a significant advantage over its competitors in the supply of data-related services.

While most submissions to the Review supported Open Banking including individuals and small businesses, some submissions questioned the value of including small businesses. Some thought that recent innovations in the small business lending market negated the need to apply Open Banking to small business lending. Others argued that banks already make data available to small business customers through accounting software providers. In consultation, the Review was advised that large accounting software providers are placing restrictions on the ability of small businesses to access their own data as a way to derive commercial benefit from the data they hold on them.

The Review has not been persuaded by the arguments to exclude access to small business information. Open Banking should significantly expand the menu of potential services available to

66. See, for example: the Financial System Inquiry (2014); the Review of the Four Major Banks: First Report (2016); and, 'Credit cards: Improving competition and consumer outcomes' — the Government's response to the Senate Economics References Committee Inquiry into matters relating to credit card interest rates (2016).
67. FSI Interim Report, pages 2-62.

small businesses, including services related to the provision of credit, and lead to better tailoring of products to their needs. That, in turn, will empower small businesses to seek out better deals at more competitive prices.

Large businesses

Larger businesses typically have better tools and greater resources at their disposal for assessing potential banking products and services. They have access to a range of bespoke products and services that are not available to small businesses, including those outside of the traditional banking sector (such as direct access to capital markets). In other words, they are generally, but not always, well-placed to obtain access to data, and know which banking products or service would best meet their requirements. They may not therefore need Open Banking.

In consultations, some banks argued that the financial affairs of large businesses may be too complex to be easily amenable to data sharing under Open Banking.

On the other hand, there are always difficulties created when policy carves in, or carves out, certain groups. Many questions arise such as: which definition of small business should be used (based on employee numbers, or turnover)?; how will the data holder identify whether the business qualifies, especially if there are aggregation rules, or 'grandfathering' eligibility through changes in status? And, any form of regulatory complexity adds unnecessary costs and can lead to unintended consequences.

In practice, by choosing to specify the relevant accounts and other products in Recommendation 3.2, it is unlikely that any of the complex or special products banks are concerned about would be the subject of Open Banking. Thus, actually carving a set of customers out of scope could prove to be an additional cost, not a cost-saving.

For these reasons, the Review has concluded that it would be ideal for all customers to have access to Open Banking.

Recommendation 3.7 – application to accounts

The obligation to share data at a customer's direction should apply for all customers holding a relevant account in Australia.

Who should be required to share data?

As the starting point for this Review is Open Banking, it follows that entities authorised to carry on banking business in Australia (i.e. authorised deposit-taking institutions, referred to as ADIs) should be subject to the core requirements.[68] There should, however, be some specific or time-limited exceptions to this rule.

Those ADIs that are listed as branches of foreign banks by the Australian Prudential Regulation Authority (APRA) should be excluded from the Open Banking requirements. Since they are not authorised to take initial retail deposits of less than $250,000 and are concentrated on wholesale banking operations, extending the obligations to branches of foreign banks would not be consistent with the objective of providing opportunities to the general public. Similarly, subsidiaries of ADIs that are not carrying on a banking business in Australia, such as wealth management or insurance arms, should also not be made automatically subject to Open Banking, as they do not generally hold banking data.

Open Banking may impose certain transitional costs on banks through changes to systems and processes, compliance and staff training. An argument could be made that all banks, irrespective of size, should be subject to Open Banking from commencement to provide a 'consistent customer experience'. Smaller banks have argued that any fixed costs will be felt by them disproportionately, and that larger banks have relatively more scope to absorb the costs of implementation. Nevertheless, customers of smaller banks would be disappointed to be denied access to Open Banking indefinitely.

The Review considered these arguments and is persuaded that the best approach is to phase in the application of Open Banking to ADIs, beginning with the largest banks. The phased implementation approach is consistent with the general objective of increasing competition (and reducing concentration) in the banking sector. Smaller ADIs may choose to opt in ahead of their scheduled phase-in date.[69]

Recommendation 3.8 – application to ADIs

The obligation to share data at a customer's direction should apply to all Authorised Deposit-taking Institutions (ADIs), other than foreign bank branches. The obligation should be phased in, beginning with the largest ADIs.

Once banking data is transferred by the customer's bank to a data recipient the notion of it being still *banking* data becomes strained. At best it is data that met the description while it was in the hands of the bank, but in the hands of the third party it is not a record of banking transactions with *them*. However, it would seem unfair if banks were required to provide their customers' data to data recipients such as FinTechs or non-bank credit providers, but those data recipients were not required

68. The term ADI means a body corporate in relation to which an authority under subsection 9(3) of the *Banking Act 1959* (the authority to carry on banking business) is in force. APRA's list of ADIs is available at: http://www.apra.gov.au/adi/Pages/adilist.aspx
69. Details of phasing in are dealt with in Chapter 6.

to reciprocate in any way, merely because they were not banks and therefore did not hold 'banking' data. An Open Banking system in which all eligible entities participate fully — both as data holders and data recipients — is likely to be more vibrant and dynamic than one in which non-ADI participants are solely receivers of data, and ADIs are largely only transmitters of data. On the other hand, this proposal is essentially about *banking* data and any concern for fairness that leads to a principle of reciprocity should not be allowed to unduly extend the scope of the system by stealth.

This concern for balancing obligations of participants has led the Review to the conclusion that, in principle, any non-ADI entity that participates in Open Banking as a recipient of data should also be obliged to provide *equivalent* data in response to a direction from a customer. Equivalent data would consist of: data received from another participant in Open Banking; any customer-provided data (subject to the exclusions discussed above); data relating to the lending of money on credit; and data relating to the payment of monies to which they are either a party or that they are facilitating. Determining equivalent data for data recipients whose primary business is not in financial services can be complex, particularly if the data recipient's sector is not yet included in the CDR. Accordingly, the Review recommends that, as part of the accreditation process for data recipients that do not primarily operate in the banking sector, such as data recipients from the technology sector, the competition regulator should determine what constitutes equivalent data for the purposes of participating in Open Banking.[70]

Recommendation 3.9 – reciprocal obligations in Open Banking

Entities participating in Open Banking as data recipients should be obliged to comply with a customer's direction to share any data provided to them under Open Banking, plus any data held by them that is transaction data or that is the equivalent of transaction data.

Who can receive shared data?

Enhancing competition and innovation would be made harder if only banks could receive banking data — the playing field must be broader. Yet customers' trust in the security of data sharing could be undermined if untrusted or fraudulent parties were to receive data.

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

Submissions have almost universally advocated some form of assessment and accreditation before non-banks should be allowed to participate in Open Banking. The challenging question is: how stringent do the security and governance standards need to be? While this is discussed in detail in Chapter 2, it is clear that institutions that are trusted to deal *with* money itself should also be trusted to deal with data *about* money. Other participating entities should be required to establish that they can safely deal with their obligations in relation to data (which may not necessarily be as stringent as

70. Accreditation is discussed in Chapter 2.

the prudential obligations for banks). The standard that non-ADIs may be required to meet should be based on the potential harm to customers, and risk to the Open Banking system, that the relevant data set and that participant pose.

Recommendation 3.10 – eligibility to receive data

Authorised Deposit-taking Institutions (ADIs) should be automatically accredited to receive data under Open Banking. A graduated, risk-based accreditation standard should be used for non-ADIs.

Recovering the costs of data transfer

Some submissions to the Review suggested that data holders should be able to charge for transfers of customer data under Open Banking. Without the ability to charge, they argue, data holders would not be fairly compensated for the costs they incur in collecting, storing and protecting customer data, and for developing the capability to respond to customers' instructions to share their data with other parties. And, the argument goes, since data recipients may benefit commercially from gaining access to customers' data, not allowing data holders to charge for data transfers would introduce a competitive distortion.[71] The Productivity Commission has also pointed out that allowing data holders to charge for data transfers may discourage spurious or malicious data transfer requests.[72]

Other submissions argued that any data that is currently made available to customers free of charge already (i.e. via internet or mobile banking) and that is in its basic or 'raw' form should continue to be made available free of charge under Open Banking. They assert that, while data holders make substantial investments in data capture and storage, this investment is made for data holders' own internal purposes and to ensure compliance with the privacy laws.[73]

In order to decide which view should be preferred, it is useful to consider what the costs actually are. An additional 'cost' for banks under Open Banking might consist of the cost of transferring the data in a particular way. This cost can be separated into its components of transition costs and ongoing costs. Transition costs would involve the cost of developing a mechanism to transfer data in a form that facilitates use by the data recipient (if that is not already being done). These costs could be kept to a minimum if the design of the transfer mechanism is simple and does not require the adoption of particular, expensive, technology.[74] When distributed over a broad client base, they should be small.

Ongoing costs would be the difference between the cost of providing data in the current form, compared to the future form for any given client, plus the cost of responding to the expected increase in the number of requests. Conceivably, the first of these might also represent a saving where the transfer under Open Banking is electronic, rather than, say, in paper form. The second could occur now, if the data was available in a more useable form. Further, some consultations have

71. See, for example, ANZ submission, page 39, NAB submission, page 16.
72. PC Data Report, page 221.
73. See, for example, FinTech Australia's submission, page 36.
74. See Chapter 5 for how this might be done.

revealed that establishing some accessible standards around the data transfer mechanism should reduce costs compared to a series of bespoke bilateral negotiations.

Data recipients will also incur costs involved with storage and protection of customer data. However, these should be small, particularly given the increasing accessibility of external data storage solutions for data recipients. And, for non-ADIs, it will be the recipients' choice whether to participate.

Recommendation 3.11 – no charge for customer data transfers

Transfers of customer-provided and transaction data should be provided free of charge.

Costs of identity verification

A possible exception to the finding that charging should not apply is the sharing of data related to identity verification. As per Recommendation 3.4, the Review proposes that data holders should be obliged, at the customer's direction, to share the *outcomes* of identity verification assessments with data recipients (subject to amendment of the AML laws).

While banking institutions do not typically compete on identity verification, there is a resource cost involved in conducting identity verification assessments and, if others benefit from that effort, it seems reasonable that their costs be defrayed. However, allowing cost recovery assumes that the cost of identity verification has not been passed back to the original customer indirectly through margins in other fees and services. In most cases banks' costs are recovered in their margins and it would be surprising if this cost element was singled out by banks for different treatment.

Further, if recovery of costs for Open Banking data transfers were allowed, calculation of those costs needs to be considered carefully. The correct amount to be recovered would be the marginal cost of that activity, rather than the set up cost of the entire system averaged across the number of customers. Otherwise, costs would escalate every time an identity check on a customer is shared and over time would cascade and could accumulate to outweigh any benefits to customers. Limits on charging would need to be contrived by requiring those charges only be recovered by the entity that performed the original verification once (rather than every time), or in other ways.

However, a case for a charge would more clearly exist if the risk to the original verifier increased as a result of others' reliance on it. Provided that the liability borne by the original verifying entity does not multiply as the outcome of their identity verification assessment is passed around the system, the original verifying entity will have incurred the costs of performing the verification regardless of whether or not they are subsequently instructed to share it under Open Banking. As such, the argument for recovery of the cost of transfer only extends to the marginal cost of the transfer, which should be virtually nothing per individual transaction.

Given implementation of the recommendations from the statutory review of the AML/CTF regime is ongoing, and the outcomes of that implementation are currently underway and the Attorney General's Department is consulting with stakeholders (including on the question of reliance), the Open Banking Review can only provide a contingent recommendation on this point.

Recommendation 3.12 – transfers of identity verification assessment outcomes

Provided that the liability borne by the original verifying entity does not multiply as the outcomes of identity verification assessments are shared through the system, those outcomes should be provided without charge.

Chapter 4: Safeguards to inspire confidence

This chapter examines potential risks posed by Open Banking, considers existing legal protections that apply and identifies the additional safeguards required to support the application of the Consumer Data Right in the banking sector. This chapter also considers the principles that should underpin a liability framework for Open Banking so that transparency and certainty can be built into the system from its inception, by design.

Customer confidence is critical to the success of Open Banking. Customers need to trust that the right safeguards are put in place to ensure that an innovative data industry does not come at the cost of customers' rights to confidentiality. Customers also need to be confident that Open Banking is focused on giving them control of their data, that data recipients will take appropriate security measures to protect that data and that there are remedies available for losses that may be suffered. Without confidence about those factors, broad customer take-up of Open Banking will be limited and the initiative may not achieve its policy objectives.

Australians are concerned about their online privacy. In 2017, a survey conducted by the Office of the Australian Information Commissioner (OAIC) revealed that many Australians regard online services as being a significant risk. Further, many Australians say they are reluctant to provide their financial details and most remain concerned about their personal information being sent overseas or shared with other organisations. However, financial institutions in Australia are highly regarded by Australians as organisations they can trust with their personal information.[75]

Banks incorporated in Australia are highly regulated and are required, as part of their prudential, regulatory and legal obligations, to manage their data and security risks. Further, the common law duty of confidentiality that is a fundamental part of the banker-customer relationship has been well established for nearly a century,[76] and is acknowledged in the Code of Banking Practice. In addition to the duty of confidentiality, banks are required to comply with the *Privacy Act 1988* (Privacy Act), which governs how they may collect, use, disclose and store personal information about their customers. These obligations have led to banks investing significant resources in building and maintaining security systems to safeguard their customers' money and information.

Submissions overwhelmingly highlighted that Open Banking needs to have high regard to data security to ensure that customers' privacy and confidentiality are maintained. Submissions further identified the importance of placing a customer in control of their Open Banking experience through their directions on which data is shared, who that data is shared with, the purpose the data can be used for and the duration of the sharing arrangement.

75. Australian Community Attitudes to Privacy Survey available at: https://www.oaic.gov.au/engage-with-us/community-attitudes/australian-community-attitudes-to-privacy-survey-2017
76. This duty of confidentiality extends to both information that has been supplied by the customer to the bank and information gathered by the bank in the course of its banking business.

Addressing the risks in Open Banking

In submissions several banks emphasised increased risk to the privacy and security of customers' banking data under Open Banking.[77] However, too great an emphasis on privacy and security could delay or even undermine the effective introduction of Open Banking. It is therefore important that the nature and character of the potential risks be examined objectively and that the risks and opportunities are adequately balanced in designing the system.

At the outset it should be noted that, despite the surveys cited earlier, many customers already consent to share their banking data with a range of third parties, including credit bureaux, providers of accounting services, and personal financial management tools. While more widespread data sharing under Open Banking may increase the *degree* of risk associated with customer banking data — with one exception — the *types* of risk under Open Banking should not differ from those that exist under current data sharing arrangements and practices.

If Open Banking achieves its objective of making it easier for customers to share their data, it will be held by more entities than is currently the case. More points of storage will increase the number of potential stages at which data can be compromised — by being hacked or subject to unauthorised access or disclosure. Similarly, transferring data more often increases the possibility of that data being intercepted or inadvertently sent to an unauthorised party, or the wrong data being sent to an authorised party.

Another potential risk under Open Banking is through the development of a common standard for data transfer (see Chapter 5). This could provide a single focal point for malicious actors to develop the means by which they could launch concerted attacks against banks and other data holders' systems. This risk needs to be mitigated by adopting robust standards for data transfer and storage which can adapt and evolve with changing technology and circumstances.[78] The Open Banking framework recommended by this Review does not propose any centralised store of all customers' banking data.[79] Accordingly, this means that another risk which is often highlighted, being the creating of a single 'honeypot' of data to attack, should be avoided.

Banks currently have very high standards of security over their data, partly as a result of the high standards of security they are expected to adopt for the protection of customers' money, and the degree of scrutiny applied to them by their banking regulators. However, it may not be necessary for smaller Open Banking data recipients to match the standards set by banks precisely. This would particularly be the case if the risks associated with the customer data they deal with are lower than the risks which the banks are seeking to manage (which, as noted above, arise because they hold customers' money, as well as their information). A risk-based approach in assessing the required security standards is important. Imposing unreasonably high standards on all participants may restrict the number of entrants, thereby limiting the ability of Open Banking to deliver substantial benefits for customers, through competition, innovation and convenience. Indeed, submissions from

77. See, for example, NAB submission, page 12; Westpac submission, page 3.
78. This aspect is discussed further in Chapter 5.
79. This alternative model would require that a single central entity be established to receive, hold and distribute all customers' banking data, acting as a clearing house.

some banks have acknowledged that it may not be reasonable to expect that smaller third parties adopt equivalent security protocols to the banking industry. For example:

> *While it may not be appropriate for third parties to establish equivalent security protocols to the banking industry, measures do need to be implemented to ensure that the vulnerability of third parties holding sensitive financial and identity data is appropriately managed and reduced, in line with community expectations of privacy and security credentials.*[80]

Another source of risk identified in submissions[81] revolved around *informed* customer consent. Ensuring that consent is genuinely informed is becoming increasingly difficult in the 'big data' and digital age.[82] Many customers are unlikely to be fully aware of how much data is being collected about them and used, as it is common practice for customers to simply accept terms and conditions of service (by clicking on 'I agree' on a screen), without fully understanding what they are agreeing to, or having any real choice but to agree if they want the service.

Reducing risks over the longer term

In considering the potential for risk in connection with Open Banking, it is necessary to also consider the existing risks which Open Banking would reduce. For example, Open Banking potentially provides a more secure way of sharing data than through processes such as 'screenscraping'.[83] The Review has been told from various sources that potentially millions of Australian bank customers have currently given their account login and password details to data recipients that then 'scrape' data from customers' internet banking interfaces and use it to, for example, identify banking products that might better suit a customer's needs, or provide personal financial management services. In some cases, the customers have agreed to grant 'write' access as well as 'read' access, effectively giving the data recipient the capability to transact on a customer's behalf.

The current legal position regarding liability for the consequences of providing account login credentials to a screenscaper is unclear. On screenscraping, ASIC's submission stated:

> *While we have not formed a definitive view, such actions could be viewed as the consumer breaching the standard banking terms and conditions for non-disclosure of passwords to third parties and passcode security requirements in the ePayments Code.*[84]

---

80. Westpac submission, page 17.
81. See, for example, submissions from ABA, Australian Payments Council, CBA, Consumer Action Law Centre, Financial Rights Legal Centre and Financial Counselling Australia, Customer Owned Banking Association, King & Wood Mallesons, and Westpac.
82. This has been noted by the OAIC in their submission to the Productivity Commission's *Issues Paper for the Inquiry into Data Availability and Use* and the Privacy Commissioner of Canada in the Office of the Privacy Commissioner of Canada's 2016-2017 Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act.
83. Screenscraping involves allowing third parties to access bank accounts on a customer's behalf using the customer's access credentials (such as their internet banking username and password). Once access to the customer's account is obtained, data is 'scraped' from the online interface and, in some cases, that access is used to initiate transactions on the customer's behalf. See further explanation in Chapter 5, Box 5.2.
84. ASIC submission, page 30.

Moreover, it is debateable whether all customers are aware of precisely what they've done in providing their login details in this way. In some cases the way in which a request for a customer's bank login details is made means that customers may not even be aware they have given their login details to someone other than their bank.[85]

That customers have been willing to provide their details provides evidence that there is a demand for value added services which require access to account information. Over time, the ability to share customers' banking data in a more seamless and secure way through Open Banking should reduce the need for customers to compromise their security and privacy by disclosing their login credentials.[86] This reduction in risk has been noted in a number of submissions.[87]

Safeguarding the privacy of individual customers

The Privacy Act

The Privacy Act is the central *legislative* framework for regulating the handling of personal information about individuals, including within the financial sector.[88] The Privacy Act requires businesses to take reasonable steps to protect personal information they hold from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

Personal information as defined in section 6 of the Act is 'information or an opinion about an identified individual, or an individual who is reasonably identifiable'. The Privacy Act contains 13 Australian Privacy Principles (APPs) that govern how entities must collect, use, disclose and store information about their customers. The APPs are designed to ensure that businesses protect the personal information of their customers to reflect the information lifecycle from planning, collection, use and disclosure, quality and security, access and correction.

The personal information of one individual can also be the personal information of another person or persons. Accordingly, some banking data from a joint bank account will be the personal information of each of the account holders and will therefore be protected by the Privacy Act.[89] Joint bank accounts are discussed in greater detail below.

The Privacy Act also regulates consumer credit reporting separately under Part IIIA, supported by the *Privacy Regulation 2013* and the industry-developed *Privacy (Credit Reporting) Code 2014*. Part IIIA regulates the handling and exchange of credit information, including the circumstances in which credit providers or reporting bodies can collect or share banking data about individuals.

85. For example, this could happen if the customers are presented with screens bearing their bank's logo to which they input their login details, without it actually being their bank's website.
86. It is possible that until Open Banking develops, some of this risk could be managed by customers being able to request 'read only' passwords from their banks so that only this password was provided for screenscraping. However, this would only be a short term solution.
87. See, for example, submissions from ASIC, CBA, Cuscal, and Verifier.
88. Other legal frameworks for protecting confidential information are discussed later in this chapter. These are important for information which is not the information about an individual.
89. It follows that each party to a joint account will be able to access the information.

Remedies for breach of Privacy Act

The OAIC is the independent statutory authority responsible for regulating the handling of personal information under the Privacy Act. The Privacy Act confers a range of functions and regulatory powers on the OAIC to promote and enforce compliance, handle complaints, and conduct investigations.

The Information Commissioner has the power to investigate a matter following a complaint by an individual. The Information Commissioner also has the power to initiate an investigation, for example following a data breach.

The OAIC has enforcement powers to:

- accept an enforceable undertaking
- make a determination (e.g. to pay compensation)
- bring proceedings to enforce a determination
- apply to the court for an injunction, or
- apply to the court for a civil penalty order of up to $360,000 for individuals and $1.8 million for companies for a breach of a civil penalty provision.

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.

Degree of sensitivity of personal information

The Privacy Act places higher protections — such as requiring entities to obtain specific consent or to take more rigorous steps to protect information — on the handling of sensitive information and government-related identifiers. Sensitive information includes information or an opinion (that is also personal information) 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 or trade union, sexual preferences or practices, or criminal record.[90] Health information, genetic information, biometric information that is to be used for certain purposes and biometric templates are also considered to be sensitive information.

The banking data of an individual is not designated specifically as 'sensitive' information. However, to the extent that it may reveal sensitive information about an individual, it would attract a higher level of protection under the Privacy Act.

90. Section 6 of the Privacy Act.

Ensuring coverage of the Privacy Act in Open Banking

The Privacy Act applies to all businesses and not-for-profit organisations with an annual turnover of more than $3 million. Small business operators with a turnover of less than $3 million are not subject to these privacy laws unless an exception applies, or the small business operator has chosen to be subject to the Privacy Act and the APPs. Both FinTech Australia and the banks have identified this gap in the application of the privacy laws and submit that all data recipients in Open Banking, regardless of their turnover, should be subject to the Privacy Act.[91]

As the Privacy Act provides the legislative framework for protecting personal information, it follows that all data recipients ought to comply with the privacy laws. Mandating that all data recipients be covered by the Privacy Act would provide a baseline for ensuring that participants implement practices, procedures and systems to safeguard their customers' personal information. Moreover, it will give customers' certainty that the enforcement mechanisms and remedies available under the privacy framework will apply in the event of a privacy breach.

Recommendation 4.1 – application of the Privacy Act

Data recipients under Open Banking must be subject to the Privacy Act.

Australian Privacy Principles in the context of Open Banking

The APPs set out high-level objectives and principles which provide businesses with flexibility to tailor their systems and processes to their needs and to the needs of their customers. The APPs are principles-based and intended to be technology neutral in order to adapt to continually changing and emerging technologies.

The Review has considered how the privacy protections would apply in the context of Open Banking in the table below. The Review has considered that express customer consent should be required, rather than leaving it to the discretion of the data recipient to determine how banking data is collected and dealt with under Open Banking. This would require a modification of the privacy protections, as set out below.

91. ANZ submission, page 31 and FinTech Australia submission, page 31.

Table 4.1 Modifications of privacy protections for Open Banking

Australian Privacy Principle	Brief description of APP	Application to Open Banking	Suggested privacy protection modifications
APP 3 – Collection of solicited personal information	APP 3 outlines when and how an entity may collect personal information that is solicited from an individual or another entity.	APP 3 does not require informed and express consent from the customer. All that is required under APP 3 is for the data recipient to demonstrate that the collection of personal information is reasonably necessary for the data recipient's functions or activities. For sensitive information, a data recipient must demonstrate that the individual concerned consents to the collection. APP 3 requires an entity to collect personal information directly from the individual unless an exception applies.	Before a data recipient can collect a customer's banking data, the data recipient must be able to demonstrate that express consent has been received from the customer. The new Consumer Data Right will allow a customer to direct that their data holder transfer their personal information to a data recipient. This means that an exception for Open Banking will be required to ensure that a data recipient is able to receive personal information from a data holder rather than directly from the individual.
APP 4 – Dealing with unsolicited personal information	APP 4 outlines the steps an entity must take if they receive unsolicited personal information.	If a data recipient receives unsolicited personal information, APP 4 requires the data recipient to decide whether it could have collected the information under APP 3.	This Review recommends that express consent be required under APP 3. This means that a data recipient who has received unsolicited banking data will need to either seek express consent or be required to destroy or de-identify the unsolicited personal information.
APP 5 – Notification of the collection of personal information	APP 5 sets out the matters an entity must make an individual aware of when collecting that individual's personal information.	APP 5 requires data recipients to take reasonable steps to notify the individual of certain matters. For example, a data recipient should notify an individual of the purposes of collection and whether the entity is likely to disclose personal information to overseas recipients.	A data recipient should be required to notify customers of the purpose for which they have collected their data. In particular, customers must be notified of uses such as marketing and the on-sale of a customer's data, as well as sending the customer's data overseas. A data recipient should not be able to rely on the reasonable steps test for Open Banking, as currently permitted.

Australian Privacy Principle	Brief description of APP	Application to Open Banking	Suggested privacy protection modifications
APP 6 – Use or disclosure of personal information	APP 6 provides that an entity can only use or disclose personal information for a purpose for which it was collected (primary purpose), or for a secondary purpose if an exception applies.	If a data recipient wants to use a customer's banking data for another purpose (secondary purpose), the data recipient must either receive consent or be able to demonstrate that the customer would reasonably have expected their information to be used for that secondary purpose. That secondary purpose must be related to the primary purpose of collection. If a customer's banking data is considered to be sensitive information then the secondary purpose would need to be directly related to the primary purpose.	A data recipient should demonstrate that any secondary use is directly related to the primary purpose. This promotes customer confidence that their banking data will not be misused or dealt with in a way they did not envisage.
APP 7 – Direct Marketing	APP 7 provides that an entity must not use or disclose personal information it holds for the purpose of direct marketing unless an exception applies.	Before a data recipient can use a customer's banking data for marketing purposes, the data recipient must meet specific conditions. Importantly, the customer must reasonably expect the data recipient to use or disclose their banking data for a direct marketing purpose. If a customer's banking data is considered to be sensitive information, a data recipient can only directly market to the customer if the customer has consented.	To ensure that customers are not marketed to inappropriately, the Review recommends that express consent (which is not bundled with other consents) be required by the customer before a data recipient can directly market to the customer.
APP 8 – Cross-border disclosure of personal information	APP 8 deals with the disclosure of personal information to overseas recipients, and who is accountable if the overseas recipient breaches the APPs.	Before a data recipient can disclose a customer's data to an overseas recipient, the data recipient must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the data. APP 8 does not require a data recipient to seek customer consent prior to disclosing the data to an overseas entity.	Express customer consent should be specifically sought before a data recipient sends a customer's banking data overseas.

Recommendation 4.2 – modifications to privacy protections

The privacy protections applicable to Open Banking should be modified as suggested in Table 4.1.

Security of personal information

Australian Privacy Principle 11 requires the protection of personal information from interference, misuse and loss, unauthorised access, modification and disclosure. APP 11 further provides that if an entity no longer needs the information for any purpose then they must take reasonable steps to destroy or de-identify the personal information. Whether personal information is destroyed or de-identified is at the discretion of the entity holding that information.

This requirement to destroy or de-identify information is relevant to Open Banking given a customer will be able to readily withdraw their consent or limit the time in which a data recipient can receive their banking 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. However it is important to note that, under the Privacy Act, individuals have no right to instruct deletion of their personal information. The right to deletion was considered by the PC's Interim Data Report which concluded they were not convinced of the public benefit or of the practicality of a right to delete.

The Review considered the possible right to deletion in light of the EU's new right to erasure ('right to be forgotten') under the General Data Protection Regulation which will become law in May 2018. However, it quickly became clear that the right to deletion and its legal implications are a much broader issue beyond the scope of Open Banking. Any development in this regard should be part of a more general consideration of Australian privacy law.

Recommendation 4.3 – right to delete

Given the many complexities involved in legislating for a right to deletion (including the range of legal obligations to retain records) and the fact that individuals currently have no right to instruct deletion of their personal information under the Privacy Act, it is beyond the scope of Open Banking to mandate a special right to deletion of information.

Keeping customers' data confidential

The common law

As some business customers' data may not be personal information, the Privacy Act will not cover all of the data involved in Open Banking. Accordingly, remedies for privacy breaches for some businesses will lie under the common law. The common law imposes a contractual duty of confidentiality on banks not to disclose the affairs of their customers — whether individuals or businesses — unless the disclosure falls within four limited exceptions.[92] In addition, the law of equity can impose an obligation on banks to maintain confidence.[93] Further, an obligation to treat customer's information confidentially is often included as a condition in the contract a customer has with their bank for services.[94] These obligations of confidence extend to all types of customers and therefore give business customers a claim against their bank if their information is not kept secure.[95]

Compensation for breach of confidentiality duty

Customers seeking compensation for a breach of the common law duty of confidentiality are able to take their dispute through the court system or an alternative dispute resolution mechanism (if available).

Access to compensation is particularly important for customers who are financially constrained in their ability to take their disputes through the court system. These would be individuals or small businesses. As noted above, for individuals there is a well-established privacy dispute framework that offers individuals with a low-cost option to resolving their disputes. Small businesses may have access to a dispute framework under the *Corporations Act 2001* (Corporations Act). The Corporations Act requires that holders of an Australian Financial Services Licence (AFSL) must have a dispute resolution system available for their 'retail clients'. This must consist of:

- internal dispute resolution procedures that meet the standards or requirements made or approved by ASIC, and
- membership of one or more ASIC-approved external dispute resolution schemes.

For this purpose, two ASIC–approved external dispute resolution schemes currently operate in the Australian financial and credit sector. They are the Financial Ombudsman Service and the Credit and Investments Ombudsman. This means that these external dispute resolution schemes are available to small businesses (and individuals) that are 'retail clients', being small businesses with less than 20 employees.[96] If the data recipient is not the holder of an AFSL, the office of the Australian Small Business and Family Enterprise Ombudsman also provide assistance to small businesses and are able to provide access to external alternative dispute resolution services.

---

92. *Tournier v National Provincial and Union Bank of England* [1924] 1 KB 461. This duty of confidentiality is implied into the contract between a bank and its customer. The exceptions include where the disclosure is made with the express or implied customer's consent, is required by law, is necessary for the fulfilment of a public duty or is necessary to protect the legal rights of the bank.
93. The equitable duty of confidence applies to information which is of its nature confidential and is provided in circumstances where the recipient could reasonably expect to have realised that it was under an obligation to keep the information confidential.
94. Acknowledgement of such a term is included in the Code of Banking Practice.
95. These rights are also available to individuals, in addition to any rights under the Privacy Act.
96. As a general rule, the 'retail client' definition in the Corporations Act is complex.

For larger businesses, the way to seek compensation for a breach of confidentiality is to go through the court system.

Recommendation 4.4 – dispute resolution for small business

Small business customers should be given access to internal and external dispute resolution services for confidentiality disputes similar to those that exist for individuals under the Privacy Act.

Giving customers control

Under the model of Open Banking recommended by this Review, a customer initiates a data sharing arrangement by directing the holder of their banking data to share their data with a third party – the data recipient. As part of that direction, the customer should be able to give specific instructions on what data is shared, who that data is shared with, and the duration of the sharing arrangement. This direction can be seen as a form of consent by the customer to the provision of their data to the data recipient. Separately the customer should have arrangements with the data recipient that should include consent to the purpose the data can be used for.[97]

This use of consent in Open Banking is important because consent is a fundamental concept in the Privacy Act and is relevant to the operation of a number of the Australian Privacy Principles (APPs). Under the APPs, consent is framed as both a basis to authorise the treatment of personal information in a particular way and as an exception to a general prohibition against personal information being treated in a particular way. Consent can be express or implied and the Privacy Act does not specify the form in which consent must be received from an individual. Consent can also be bundled together to allow entities to obtain consent for a wide range of collections, uses and disclosures of personal information.

Some submissions raised concerns with the breadth of consent permitted under the Privacy Act being applicable to Open Banking. They argued that customer consent in Open Banking should be:

- freely given
- express, rather than implied
- informed
- specific as to the purpose (when requested by a data recipient)
- time limited, and
- easily withdrawn with immediate effect.[98]

97. It is not necessary for a data holder to be part of the arrangements with the data recipient on the purpose for which the data can be used. As noted below, it is the data recipient, and not the bank, that should be responsible for complying with that purpose.
98. See, for example, submission from Australian Privacy Foundation, ANZ, ASIC, ABA, Australian Payments Council, CBA, Cuscal, Customer Owned Banking Association, Envestnet Yodlee, FinTech Australia, King & Wood Mallesons, Moneytree, NAB, and Westpac.

Further, some submissions have noted that there are certain uses in respect of which consent needs to be clear and express for the purpose of Open Banking. These include those relating to the use of a customer's data for marketing, the on-selling or sharing of a customer's data and the sending of a customer's data overseas.[99]

This Review considers that the use of implied and bundled consent for the data provided through Open Banking could undermine the key elements of customer control, namely that: the consent is not informed; voluntarily given; current and specific; and that the individual has the capacity to understand and communicate their consent. Accordingly, this Review believes that consent for the use of banking data provided to the data recipient through Open Banking should meet the points set out above. Further, for the use cases which are particularly sensitive, consent needs to be clear, concise and effective, as well as being functional, rather than bundled with other disclosures. The manner in which this consent should be provided is discussed further below.

Such additional requirements that the consent for use of Open Banking data be expressly given, specific as to the purpose, time limited and able to be withdrawn are elements that go beyond the requirements of the Privacy Act. However, the Review supports these additional elements as they assist in safeguarding against customers' losing control over their data and, consequently, their confidence in Open Banking.

Further, a data recipient who wants to use a customer's data for a purpose other than that for which it was originally received should be required to seek that customer's further consent rather than include it as a condition of the original service.

Recommendation 4.5 – customer control

A customer's consent under Open Banking must be explicit, fully informed and able to be permitted or constrained according to the customer's instructions.

99. The Office of the Privacy Commissioner of Canada's 2016-2017 Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act noted that organisations in designing their consent process should be guided by certain principles, including: individuals should be provided with easy 'yes' or 'no' options when it comes to collections, uses or disclosures that are not integral to the product or service they are seeking; organisations should design and/or adopt innovative consent processes that can be implemented just in time, are specific to the context and appropriate to the type of interface used; and organisations should be in a position to demonstrate the steps they have taken to test whether their consent processes are indeed user-friendly and understandable from the general perspective of the their target audience.

Customer control: understanding and consent

The Review has considered how the technology adopted for customer authentication and customer consent could enhance a customer's control and understanding about how their data is being used. Technology has the potential to manage customer directions and consent in a transparent manner and should be designed in a way that allows customers to self-select:

- in giving a direction to the data holder, the accounts they choose to share data from
- in giving a direction to the data holder, the length of time the data is to be shared, and
- in giving consent to the data recipient, the purpose/s for which the data can be used.

On receiving a direction from a customer to share their data, it is in the interests of data holders to educate their customers of the implications of that request. Prior to complying with the request, data holders should notify the customer that a request to share data with a data recipient has been received and that the customer's relationship with the data recipient does not involve the data holder and the sharing of data is at the customer's own risk. Education through this notification will play an important role in ensuring customers understand that they cannot hold the data holder responsible once their direction has been made and complied with. However, it is important that the notification does not add undue friction or impede a customer's willingness to share their data. The Review therefore recommends that the notification issued by a data holder be limited in its content to a single screen or page.

Data recipients will need to facilitate a customer's ability to self-select from a list of possible uses of their data to give customers the opportunity to choose which dealings they agree to, and which they do not. In seeking consent for possible uses, data recipients should similarly be limited to either a single screen or page to avoid customers becoming disengaged or overwhelmed by the consent process. Limiting consent to one page should encourage customers to actively participate in making decisions about the use of their data so that consent is informed and meaningful.

Technology should also allow a customer to terminate a data sharing arrangement at any time through both the data holder and data recipient's platform.

Recommendation 4.6 – single screen notification

A data holder should notify the customer that their direction has been received and that the future use of the data by the data recipient will be at the customer's own risk. That notification should be limited to a single screen or page. Data recipients should similarly provide the customer with a single screen or page summarising the possible uses to which their data could be put and allow customers to self-select the uses they agree to.

Transparency in joint accounts

Joint accounts are accounts where more than one person or entity is the customer. The joint account is shared between those persons or entities, so that they are the account holders together. There are typically two types of joint accounts: where only one account holder needs to authorise transactions, and where the authorisation of more than one account holder is needed. An account that allows one account holder to authorise transactions allows all account holders to transact on the account independently of each other. An account that requires more than one account holder to authorise only allows transactions to be made if those account holders agree.

As a principle, the authorisations that currently apply to joint accounts in respect of the transfer of money should also apply to the transfer of data which ultimately relates to that money. This would mean that if a joint account requires more than one account holder to authorise a transfer of money from the account then a direction to share data relating to that account should require the consent of the same number of account holders. Also, this would mean that if a joint account requires only one account holder to authorise a transfer of money from the account then a direction to share data relating to that account (for example, information on the payments which have been authorised) should also require the consent of one account holder only. However, before this principle is implemented it will be important that customers that are joint account holders be educated and informed that the level of authorisation needed to transfer data *about* an account is the same as that needed to transfer money *from* that account.

This education and notification could be achieved in a number of ways. Banks could notify customers of a change in the terms and conditions of joint bank accounts or allow customers to self-select whether they wish to confirm that the authorisation extends to data. Banks may also wish to provide joint account holders with the option of being able to separately determine the authorisations that could apply to transfers of money and transfers of data.

Regardless of the authorisations that apply to joint accounts, it will be important that in any data sharing arrangement relating to joint accounts the system provides for each joint account holder to be notified of the commencement of a data transfer arrangement. Any account holder should be allowed to terminate the data transfer arrangements through the account holder's interface with the data holder.

Recommendation 4.7 – joint accounts

Authorisation for transfers of data relating to a joint account should reflect the authorisations for transfers of money from the joint account. Each joint account holder should be notified of any data transfer arrangements initiated on their accounts and given the ability to readily terminate any data sharing arrangements initiated by any other joint account holders.

Data security in Open Banking

Common standards for all participants

The PC Data Report recognised that robust security standards are a crucial foundation to realising the benefits of data transfer to the fullest extent. Further, the PC Data Report provided in-principle support for industry developing their industry-specific arrangements. However, the right balance needs to be struck to ensure that security standards do not act as a barrier to market entry for new start-ups and lead to lower competition.

In the UK, the Implementation Entity has released technical security standards in the areas of customer authentication, API specification and encryption. The standards are highly detailed and are prescriptive in nature. The EU's PSD2 has mandated specific requirement for managing operational and security risks, including system performance monitoring, contingency measures for unplanned unavailability or a systems breakdown, and incident management and reporting.

FinTech Australia identified in its submission to the Review that the current approach of having varying, competing security standards for basic information transfer creates substantial inefficiency, and leaves the door open for institutions to continue to use their own interpretation of baseline security standards as a means to pick and choose whom consumers are able to share their data with.

From the customer's perspective, security standards play an important role in giving customers the confidence that an objectively-determined standard has been met, regardless of which accredited data recipient they choose to transact with under Open Banking. Although compliance with security standards largely occurs behind the scenes, customers should be able to expect that their banking data will be securely transferred and held at all stages and that a failure to meet certain security standards will result in a consequence to the relevant party.

Security of data will need to feature as part of each design phase under Open Banking.[100]

Current security requirements

In addition to the Privacy Act's requirement to secure personal information, banks are also subject to APRA's prudential standards and guidance on data security. APRA Prudential Standard CPS 231 and Practice Guides CPG 234 and 245 address the risks associated with handling data and dealing with third parties.

Those standards set out APRA's expectations for regulated financial institutions to consider and address risks such as:

- fraud due to theft of data
- business disruption due to data corruption or unavailability
- delivery failure due to inaccurate data

100. See Chapter 5 for more discussion on security of data.

- breach of regulatory obligations resulting from unauthorised disclosure, and
- controls to ensure adequate data quality and data security, particularly in arrangements involving third parties.

APRA's requirements effectively set security standards for customer banking data that go beyond the requirements of the Privacy Act.

Examples of security standards

Submissions to the Review advised of a number of security standards used internationally and adopted domestically. Adopting an international standard has the obvious benefit of global interoperability which would, over time, lead to greater competition and innovation across borders.

ISO 20022

The Internal Organisation for Standardisation has developed ISO 20022 as a global and open standard for electronic data interchange between financial institutions. Notably, the RBA's New Payments Platform will be adopting the ISO 20022.

ISO 27000 series

The ISO 27000 series is a group of information security standards developed by the International Organisation for Standardisation and the International Electrotechnical Commission to provide a globally recognised framework for best-practice information security management.

NIST

The National Institute of Standards and Technology (NIST) in the United States develops and implements standards across a wide range of industries. In October 2017, the NIST and the Department of Homeland Security Science and Technology Directorate released a set of standards, known as the Secure Inter-Domain Routing to reduce the risk of electronic messages being intercepted or stolen.

Australian Government Information Security Manual

Australian Government agencies must apply the Attorney-General's Department's *Protective Security Policy Framework* and the Australian Signals Directorate's *Australian Government Information Security Manual.* These documents articulate the Australian Government's requirements for protective security and standardise information security practices across government.

Recommendation 4.8 – security standards

In order to be accredited to participate in Open Banking, all parties must comply with designated security standards set by the Data Standards Body.

Liability framework

A comprehensive liability framework for the allocation of responsibility between participants is important for the proper functioning of Open Banking. The PC Data Report advocated that in order for a data sharing framework to build community trust and confidence, it is essential to embed transparent risk management practices and explicitly deal with risk and liability. Leaving the attribution of liability to the market could result in less informed (or less powerful) parties accepting the liability risks associated with a data sharing request. For customers there is a risk that liability would be buried in a dense set of terms and conditions and therefore not readily understood and genuinely agreed. Further, a lack of clarity on liability for the failure of a participant in Open Banking could discourage active participation by data holders and data recipients.

Submissions sought clarification on how liability is to be determined for the new Consumer Data Right in the context of Open Banking. Many submissions indicate support for a comprehensive legal framework which clarifies the liability for each party to address the risks. A comprehensive legal framework is likely to obviate the need for parties to bilaterally negotiate liability risks resulting in efficiency gains. Consistency and transparency across all data sharing arrangements would provide certainty for customers on who bears the liability for any losses suffered.

Risks and liability issues include those that could arise when:

- the wrong data is transferred by a data holder
- the data transferred by a data holder is incorrect
- a data breach occurs during the transfer of data
- a data recipient fails to adequately protect data they receive
- a data recipient uses the data they receive inappropriately, and
- a data recipient fails to satisfy accreditation requirements.

Principles for a comprehensive liability framework

It is important that the comprehensive liability framework is principles-based, so that it can be applied consistently and to changes in circumstances. For the purpose of establishing these principles, existing liability frameworks can be drawn upon.

Privacy law provides one useful framework, in the context of the obligations for holding and transfer of a customer's personal information. These obligations include ensuring that a customer's personal information is:

- accurate, up-to-date and complete
- protected from misuse, interference, loss, unauthorised access, modification or disclosure, and
- corrected to ensure the information is relevant and not misleading.

Banking law — specifically, the obligations associated with the holding and transfer of money — provides another useful framework. These obligations include that a bank ensures that a customer's money is transferred only at the direction of the customer, and in accordance with that direction if it is validly given. Under this framework, as a matter of general principle, if a bank follows such a

direction, then the bank is not liable for the receiver's conduct with the money once it has been paid nor is it responsible for the relationship between the customer and the payment receiver.

The Review considered a number of case studies relating to allocation of liability between participants in the Open Banking system to determine if relevant precedents from these frameworks could apply to resolve questions of liability and these are set out in the Table 4.2. It is important to note that a number of the case studies outlined in the table below will not necessarily result in a financial liability to an aggrieved party as not every privacy breach or loss of data will require compensation.[101] Further, these cases studies relate only to the allocation of data-related liability between participants in Open Banking, not to liability between banks and customers for transactions on their accounts (for example under the ePayments Code).

Table 4.2: Liability case studies

Scenario	Application of privacy law framework[102]	Application of banking law framework[103]	Suggested result under Open Banking liability framework
The customer directs their bank to share their savings account transaction records to a data recipient. The bank incorrectly shares transactions from their credit card.	The bank could be liable to the customer as it has shared information that was not authorised. The bank has existing obligations under APP 11 to ensure that they take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.	The bank is responsible for ensuring that it properly follows the customer's valid directions in respect of transactions on the customer's account.	The bank should be liable to the customer for its sharing of incorrect information with the data recipient.
Customer A requests their bank to share their savings account transaction records with a data recipient. The bank incorrectly shares Customer B's banking data.	The bank would be liable under the Privacy Act to Customer B. The bank has existing obligations under APP 11 to ensure that they take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised	The bank is responsible for transacting on Customer B's account without a valid direction from Customer B.	The bank should be liable to Customer B for its unauthorised sharing of information with the data recipient.

101. For example, in the case of breaches of privacy obligations, the OAIC has a range of enforcement powers that range from less serious to more serious, including powers to accept an enforceable undertaking to seeking a civil penalty.
102. Responses in this column are given as if the relevant information being transferred is personal information of the customer.
103. Responses in this column are given as if the transactions in the customer's information were transactions in the customer's money.

Scenario	Application of privacy law framework[102]	Application of banking law framework[103]	Suggested result under Open Banking liability framework
	access, modification or disclosure.		
A customer directs their bank to share their banking data with an accredited data recipient. While the data is shared accurately according to that direction, the data itself misleads the data recipient to offer the customer a product and the data recipient suffers a loss.	No privacy law obligations owed to the data recipient. However, the bank would continue to comply with APP 10 and APP 13.	The bank is not responsible for the relationship between the customer and the receiver.	The bank should not be liable to the data recipient. The customer may be liable to the data recipient (in the same way as if it provided the data directly to the data recipient) depending on the terms of the contract between them.
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.	Banks are expected to comply with APP 10 and APP 13 under the Privacy Act. APP 10 requires a bank to take reasonable steps to ensure their customer's personal information is accurate, up-to-date and complete. APP 13 requires a bank to take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading.	The bank is not responsible for the relationship between the customer and the receiver. The bank could be responsible to the customer for inaccuracy of the records it keeps for its customer.	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.
A malicious actor manages to intercept the customer's data during the transmission between the bank and an accredited data recipient.	No applicable privacy law obligations.	The bank is responsible to the customer for not fully executing the customer's direction by ensuring that transaction was safely completed.	The bank should be liable to the customer for the loss suffered by the customer because of its failure to transfer the data at the customer's direction.
The accredited data recipient has received the data securely by the bank. However the data recipient suffers a data breach impacting a number of	The data recipient will be responsible for securing its systems. Under the Privacy Act, APP 11 requires an entity to protect the information from	The bank has followed the direction of its customer. It is not responsible for the relationship between the customer and the receiver.	The data recipient should be liable to their customers for the loss suffered by them as a result of their data breach. The bank should not be

Scenario	Application of privacy law framework[102]	Application of banking law framework[103]	Suggested result under Open Banking liability framework
customers.	interference, misuse and loss, and unauthorised access, modification and disclosure. The bank has not breached any of its privacy law obligations to the customer.		liable for the data breach which the data recipient suffered.
A customer has requested that their bank provide them with their banking data. The customer stores this data on their personal electronic device. The customer has not adequately secured their electronic device and their banking data is compromised.	No applicable privacy law obligations.	The bank has followed the direction of its customer. It is not responsible for the loss caused by the customer's actions.	The bank should not be liable for the customer's actions.
An accredited data recipient fails to meet the requirements for accreditation and as a result causes a number of customers to suffer losses.	No equivalent privacy law obligations.	A bank is not responsible for the failure of the recipient to meet its authorisation obligations.	The data recipient should be liable to their customers for any loss caused by their failure to meet accreditation requirements.
An accredited data recipient uses the customer data it receives for unlawful means.	The data recipient can only use or disclose personal information for a purpose for which it was collected, or for a secondary purpose if an exception applies under APP 6.	A bank is not responsible for the actions of a recipient to whom it has been validly directed to transfer data by a customer.	A bank should not be responsible for the actions of a data recipient to whom it has been validly directed to transfer data. The malicious data recipient should be liable to their customers.

The case studies in the table above are not exhaustive, but provide some examples of where a liability could arise and which party the Review considers should be held accountable and responsible. The Review considers that from these, and the underlying frameworks, a principle can be drawn that participants in the Open Banking system should be liable for their own conduct but not the conduct of other participants in the system. This means, for example, that where a data holder acts on a valid instruction from a customer to transfer the customer's data then the data holder is liable to ensure that the instruction is effected, but should not be liable for the conduct of the data recipient with that data, or the relationship between the customer and the data recipient.

Recommendation 4.9 – allocation of liability

A clear and comprehensive framework for the allocation of liability between participants in Open Banking should be implemented. This framework should make it clear that participants in Open Banking are liable for their own conduct, but not the conduct of other participants. To the extent possible, the liability framework should be consistent with existing legal frameworks to ensure that there is no uncertainty about the rights of customers or liability of data holders.

Chapter 5: The data transfer mechanism

This chapter addresses how data should be transferred under Open Banking. The usefulness of a right to access data depends on the way that data is made available. This Report, for example, would be more difficult to access if it could only be requested by phone and sent by post, rather than being available to download from a website. Consistent with the guiding principles of this Review, the data transfer mechanism needs to be customer focussed, efficient and fair, and promote confidence, competition and innovation. Other important attributes for the data transfer mechanism that have been raised over the course of this Review include security, transparency, convenience, sustainability, flexibility, robustness and 'developer friendliness'.

Communicating information can be complex (see Box 5.1).

Box 5.1: Aspects of communication

Communicating information involves many considerations. At a basic level, this includes deciding:

- what information or meaning needs to be conveyed
- how that information is encoded, and
- how it can be found, requested, and transported.

For example, this Report conveys the findings of the Open Banking Review. That information is encoded in English, which is in turn encoded in either a digital format, such as a portable document format (pdf), or as a physical (hardcopy) document. The Report can be found, requested, and transported in various ways, including on the World Wide Web (the Web). The Web uses a suite of communication protocols including the Hyper Text Transport Protocol (HTTP), the Transmission Control Protocol (TCP) and the Internet Protocol (IP). A copy of the report could also be transported via the postal system, which has its own set of protocols.

For information that is to be kept confidential there are also security considerations, including:

- authorising access for certain people
- linking their identity to credentials
- authenticating credentials, and
- securing information in transport.

For example, the identity of an individual who opens a bank account must be established under the Know Your Customer (KYC) rules of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*. Within a bank's system this identity is then linked to various credentials that individuals must present to access their account. In the case of online banking, a secure variation of HTTP called HTTP Secure (HTTPS) is used to encrypt the information as it travels over the internet between the bank's server and the customer's internet browser.

If information must be accessed by software, the 'developer friendliness' of the transfer mechanism becomes another crucial consideration, including having:

- clear documentation of the transfer mechanism
- stable version control over time, including backwards compatibility
- clear (and ideally open) licensing, and
- facilities to test software and query problems.

Access to banking information

Much of the banking information that could be subject to Open Banking is already available to customers. Information like account balances and transaction records can usually be accessed by the account holder in various ways, including via bank branches, websites, phone banking and mobile banking applications. The main problem with access is the difficulty for customers in providing their data to third parties. As noted in earlier chapters, letting customers provide their data to third parties easily and safely has the potential to greatly benefit them and the economy generally.

Currently, customers may need to share information manually, such as by downloading bank statements in a portable document format (pdf) or downloading transactions and account details as comma separated values (csv). Manual transfers are slow, time consuming, and error prone, making them particularly poorly suited to situations where the information needs to be updated regularly. It is also hard to rely on the completeness and authenticity of information provided by a customer.

Some third-party services automate access to banking information by asking customers to provide them with their login details. These credentials are then used by software that is designed to log into the customer's online banking account and interpret the information presented there for human consumption. Sometimes third parties also reverse engineer the interface that banks create to allow their own mobile app to request information.

Box 5.2: Data sharing via screenscraping

Screenscraping technology is used by many FinTech businesses to access a customer's banking data. It involves the customer providing the FinTech, or an associated 'data aggregator', with their access credentials that the FinTech uses to log into the bank's online banking interface. The technology then extracts the customer's data – such as their account balance and transactions – from the information that the customer would be able to see on the screen.

In the absence of data sharing agreements with banks that would allow them to access customer data via secure portals – such as that imagined under Open Banking – screenscraping has become the FinTech industry's default way of gaining authorised access to customers' financial data. While it has become popular, it has done so out of necessity, rather than because it is an elegant technology design for data sharing. Screenscraping is risky, unstable and costly.

- 'Risky' because screenscraping may compromise a customer's protection from fraud. Handing over login credentials to enable screenscraping may be a violation of the bank's terms and conditions, meaning the customer may be liable if their credentials were to be compromised.
- 'Unstable' because any change to a bank's online user interface, from a simple move of a button from one part of the page to another or to a complete redesign, is likely to take a screenscraping solution out of action until it can be manually fixed by a developer.
- 'Costly' because screenscraping is a relatively inefficient and clumsy way of accessing and sharing data.

Given that the handing over of a customer's login credentials goes against all the usual security advice of not giving out your passwords, FinTechs report that a significant number of potential customers withdraw at that stage in the sign up process where they are asked to provide their login credentials. Nevertheless, information presented to the Review suggests millions of Australian customers have elected to sign up to these businesses as a way to share their banking data in order to access the services they desire. FinTech businesses employing screenscraping technology provide a range of services, including: personal budgeting tools; lending to small businesses; and tools to enable consumers to find better deals on significant household expenditure items (such as gas and electricity bills).

These 'screenscraping' 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.

Often, third parties manage the problems associated with screenscraping by using 'middleware' providers that specialise in accessing bank data and re-presenting it, via a dedicated interface, for other third parties. These specialised 'complexity resolvers' limit the number of parties that need to hold a customer's credentials. They can also take advantage of economies of scale to manage the design and reliability challenges associated with screenscraping. However, at best, this is a partial solution to the access problem.

Ultimately, the problems associated with screenscraping and manually transferring data discourage customers from sharing their banking information and limit feasible use cases. Overcoming this barrier to competition and innovation is vital to the success of Open Banking.

Third parties need a dedicated interface

In the modern digital economy the typically accepted way to share information with third parties securely and efficiently is to provide a dedicated interface that third-party software can use to access the information directly. Dedicated interfaces that are designed to allow different software programs to interact in defined ways are often called application programming interfaces (APIs).

APIs are pieces of software that have been designed to help other software interact with an underlying system. APIs are similar to user interfaces (UIs), which allow people to interact with computers more easily by providing clearly defined structures and procedures. Modern computers usually use graphical user interfaces (GUIs) with features like buttons, windows, menus and a mouse cursor. However, APIs are closer to older command line interfaces (CLIs), which define a set of text commands.

Sometimes analogies are used to help explain the concept to non-technical audiences. For example, a popular video explanation describes an API as the waiter that takes information between the table (the client application) and the kitchen (the underlying software).[104] The menu, which provides a structure for requests, could also be considered part of the API.

The need for interfaces that allow software components to interact predates the advent of personal computing. Older APIs were usually focussed on solving problems for other developers. For example, a desktop application might use the WinAPI to ask the Windows operating system to draw

104. Mulesoft 2015, *What is an API?*. Available at: https://www.youtube.com/watch?v=s7wmiS2mSXY

a window on the user's screen. However, the increase in connectivity provided by the internet led to the development of APIs that focus on solving broader business problems by trading information or services between parties.

APIs are now a core part of the digital economy. The Programmable Web, which is a prominent directory of web APIs, listed 17,000 publicly-exposed APIs as of March 2017.[105] One of the most well-known APIs is the Google Maps API, which is used by millions of websites and mobile applications to access directions and location data.[106] Most cloud computing services offered by Amazon Web Services — which had around 1 million active users in 2014[107] — are provided to developers via APIs. Social media platforms like Facebook, Twitter and LinkedIn also offer widely used APIs so that third-party developers can build their own applications using the platform's data.

Many submissions to the Review have assumed or explicitly recommended that data be shared with third parties using APIs.[108] Submissions from Westpac[109] and CBA[110] recommended instead a model proposed by the ABA, where customers would initiate the transfer of data by authorising third parties via their bank's website or mobile application. The ABA's proposed approach can also be classified as an API, because it involves the creation of a dedicated interface for the automated transmission of information and permissions between a bank's systems and third-party software. To return to the restaurant analogy, a menu is still a menu even if there is only one item on it and orders must be placed at the counter. The key issue is really about how banking APIs should be designed, namely whether they should be *a la carte* or the set menu. This issue is dealt with in more detail later in this Chapter.

Recommendation 5.1 – application programming interfaces

Data holders should be required to allow customers to share information with eligible parties via a dedicated application programming interface.

Some banking APIs already exist

Although most banks do not offer publicly exposed APIs that would allow customers to give third-party developers easy access to their banking information, various banking APIs do already exist.

105. Santos W 2017, ProgrammableWeb API Directory Eclipses 17,000 as API Economy Continues Surge. Available at: https://www.programmableweb.com/news/programmableweb-api-directory-eclipses-17000-api-economy-continues-surge/research/2017/03/13
106. Google 2017, Google Maps APIs. Available at: https://developers.google.com/maps/showcase/
107. Clark J 2014, '5 Numbers That Illustrate the Mind-Bending Size of Amazon's Cloud', *Bloomberg*. Available at: https://www.bloomberg.com/news/2014-11-14/5-numbers-that-illustrate-the-mind-bending-size-of-amazon-s-cloud.html
108. See, for example, submissions from FinTech Australia, Regional Australia Bank, Radiam, Yodlee, Moneytree, and Transferwise.
109. Westpac submission, page 10.
110. CBA submission, page 4.

Many Australian banks have agreements to provide data directly to accounting software packages. This likely occurs via some form of API, but the documentation is not typically published. It may also occur through manually transferring batch information.

One of the oldest and most widely used approaches to exchanging banking information with third parties is the Open Financial Exchange (OFX) standard, which defines a data format and a communication protocol. The initial OFX specification was published in 1997 by Microsoft, Intuit and Checkfree to allow information to be freely exchanged between their applications. Currently, OFX is used by over 7,000 banks, brokerages and payroll companies, mainly in the United States. Supported features include:

- transaction data
- transfers
- payments
- investments and securities, and
- multifactor authentication.

OFX is a free and open standard, although many organisations implement a proprietary variant called QFX, which is the only file format accepted by Intuit's Quicken software, and requires financial institutions to pay Intuit a licence fee. FinTS, a longstanding German standard for exchanging banking information, also uses a similar remote procedure call (RPC) based approach.

Under older versions of OFX, third parties had to hold a customer's banking credentials directly. This design feature raises the same security risks as screenscraping, because it means that customers' credentials could be compromised if the third party suffers a data breach. However, in 2016 the OFX Consortium released a new version of the standard that avoids this problem by using a framework for delegated authorisation called OAuth 2.0.

OAuth 2.0 sets out guidelines that allow users of an application to authorise it to access information held elsewhere without giving that application their login credentials. The basic guidelines can be implemented in different ways, with varying degrees of security. However, it is a widely accepted authorisation framework used by major technology companies like Google, Amazon and Facebook and published by the Internet Engineering Taskforce (IETF),[111] which also maintains the broader set of rules and conventions that govern the internet. From a user perspective, OAuth 2.0 typically allows third party software to prompt the user for authorisation when it is needed by redirecting them to and from their bank's authorisation page. This means that there is minimal disruption to the user experience.

A significant difference between OFX and more recent banking APIs is that it uses a RPC architecture, where the client application asks the server, via the API, to perform an operation. RPC architecture can be contrasted with a representational state transfer (RESTful) architecture where requests are made for resources. The RESTful approach to designing APIs lets developers use the same conventions that underpin the World Wide Web.

111. The IETF is an international not-for-profit organisation that creates voluntary standards to maintain and improve the usability and interoperability of the Internet.

It is hard to discuss the merits of RESTful and RPC-based APIs (or even explain why the difference matters) in a way that is meaningful to non-developers. The discussion is further complicated by the fact that both REST and RPC can be implemented in different ways. For example, the approach used by OFX involves a relatively complex set of message headers, whereas a more recent RPC framework called Thrift is extremely concise.

The important point is that developers have largely embraced RESTful APIs. In 2006, 80 per cent of requests to Amazon Web Services were made using their RESTful APIs rather than their Simple Object Access Protocol (SOAP) RPC APIs.[112] Between 2008 and 2010 the percentage of RESTful APIs in the Programmable Web's directory moved from 60 per cent to 74 per cent.[113] Many businesses, such as LinkedIn, that initially used an RPC-based architecture transitioned to a RESTful approach.[114] RESTful APIs were once considered poorly suited to high security applications, but payment services providers like PayPal and Stripe now use longstanding RESTful APIs.

Recent efforts to develop Open Banking APIs generally use a RESTful approach – along with OAuth 2.0 or its predecessor as the framework for authorisation. Macquarie, which is the only Australian bank currently[115] offering an open API that provides developers with account access, adopts this approach. NAB, which provides APIs for a more limited set of information, also uses REST and OAuth 2.0.

Overseas examples of the REST/OAuth approach include French bank Credit Agricole, Spanish bank BBVA, German Bank Fidor, Singaporean bank OCBC and US-headquartered Citi, which provides read and limited write access for accounts held by its customers in a range of jurisdictions, including Australia. While these APIs all share some important features, it is important to note that they differ in the detail of their implementation. In particular, they often use different OAuth profiles and data dictionaries.

Other private sector efforts to develop industry standards for Open Banking based on OAuth and RESTful APIs include the Open Bank Project, which is a start-up consortium based in Germany, and the Durable Data API (DDA) which was developed by the US-based Financial Services Information Sharing and Analysis Center as a successor to OFX.

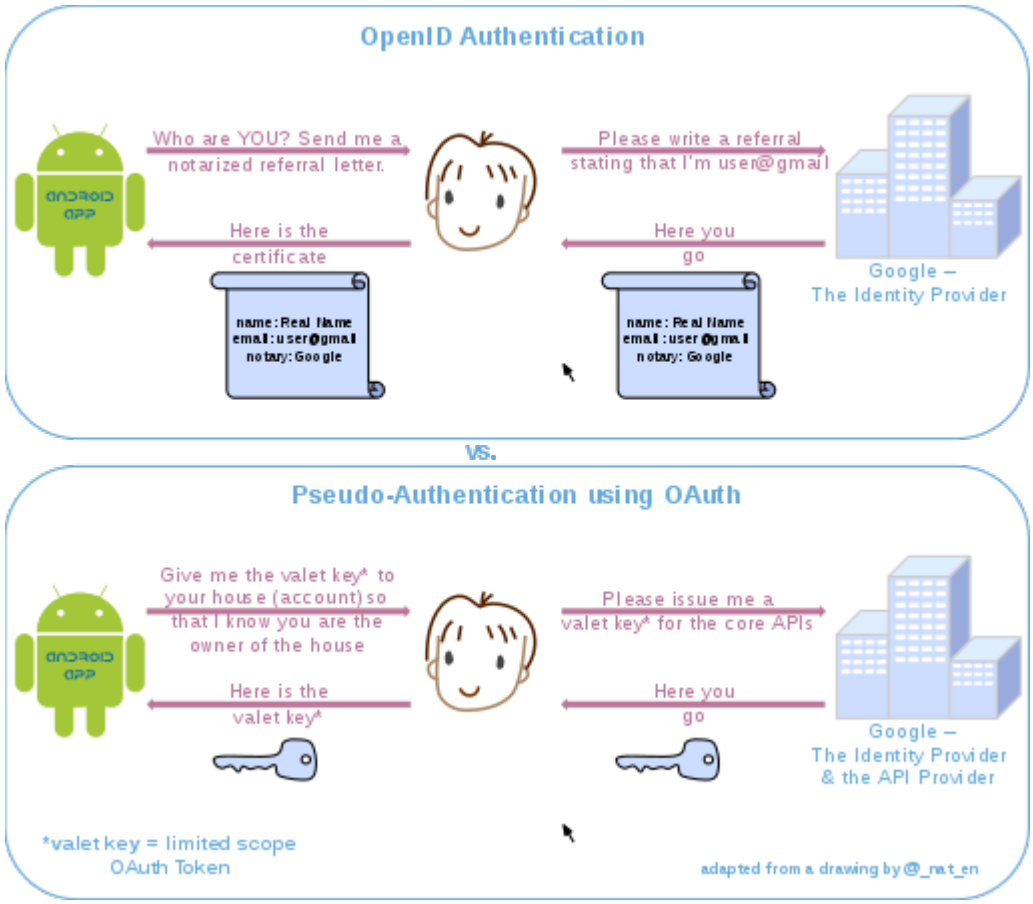
A draft Financial API (FAPI) specification has also been published by an OpenID Foundation working group. The OpenID Foundation is responsible for an OAuth 2 profile called OpenID Connect, which is widely used by companies such as Amazon, IBM, Google and Microsoft. The OpenID Connect specification standardises some of the optional elements of OAuth 2 and allows third parties to authenticate a user's identity securely (see Box 5.3). The FAPI project aims to provide a consistent means of extending the OpenID Connect specification to accommodate financial services uses.

112. Barr J 2006, 'REST vs SOAP', *AWS News Blog*. Available at: https://aws.amazon.com/blogs/aws/rest_vs_soap/
113. DuVander A 2017, 'New Job Requirement: Experience Building RESTful APIs', *Programmable Web*. Available at: https://www.programmableweb.com/news/new-job-requirement-experience-building-restful-apis/2010/06/09
114. Hartmann J 2016, 'REST vs RPC – the SOA showdown', *LinkedIn Pulse*. Available at: https://www.linkedin.com/pulse/rest-vs-rpc-soa-showdown-joshua-hartman/
115. As of November 2017.

Box 5.3: Authorisation vs authentication

The basic OAuth 2 framework allows users to authorise their bank to share information with third parties. However, authorisation (which is the process of granting permission) is distinct from authentication (which is the process of verifying identity). Authorisation can provide verification but it is analogous to a land title registry proving that an individual owns a property by handing out working keys rather than ownership certificates. In other words, it can only be used to prove identity by potentially undermining security. A further illustration of this problem is provided in Figure 5.1. There are also situations where a user may wish to authorise the sharing of a piece of information – such as their date of birth – without verifying their identity.

Figure 5.1: Authentication with OpenID vs OAuth



Source: Wikipedia

The need for technical standards for APIs

Ideally, the design of banking APIs would be driven by informed user choice and competition. The best, or most popular, solutions would win out over time.

However, relying on competition is problematic when entities are being compelled to release information that they might not otherwise provide within a prescribed timeframe, as is the case when a government mandates that certain data must be disclosed. Although financial institutions have largely welcomed the prospect of Open Banking, conflicts between their commercial considerations and the interests of consumers could easily arise. For example, institutions with legacy architecture may choose an approach that minimises their internal costs while increasing the

costs for third parties. The cost of retraining and updating legacy systems means that software choices often create lock-in effects. This is particularly likely to be true in an industry such as banking, which is highly concentrated and where consumers rarely change providers.

Setting standards overcomes the problems associated with relying on competition to drive the adoption of best practice banking APIs. The development of a standard approach does not prevent institutions from implementing an additional alternative if they believe that the standard can be improved on. If the proposed standard is poor, third parties may avoid Open Banking altogether by continuing to rely on screenscraping.

Chapter 2 of this Report provides a more detailed discussion of the need for standards and how the risks associated with a standards-based approach can be addressed.

Other jurisdictions' technical standards

Australia is not the first jurisdiction to face the challenge of developing technical standards to support the implementation of a broader requirement to grant third-party access to banking data. Transferring data securely and efficiently is also not a new problem, so Australia can look to approaches that have already been proven in banking, and in other contexts.

The EU sets functional requirements

In 2015, the European Union (EU) passed the second Payment Services Directive (PSD2), which, among other things, requires that banks allow payment initiation and account data retrieval by competent third parties, including specifying that they must treat payment orders and data requests without discrimination and make payment initiation available.[116]

PSD2 also requires the development of a regulatory technical standard (RTS) for authentication and communication between account providers and third parties, having regard to:

- ensuring an appropriate level of security through the adoption of effective and risk-based requirements
- ensuring the safety of funds and personal data
- securing and maintaining fair competition
- ensuring technology and business-model neutrality, and
- allowing for the development of user-friendly, accessible and innovative means of payment.[117]

116. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, Articles 66 and 67. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366
117. See Article 98.

Given the directive of ensuring technology neutrality, the RTS focuses on functional requirements. In summary, the draft RTS (which is yet to be endorsed by the European Parliament) requires that:

- account providers offer at least one secure communication interface with third parties
- third parties be able to rely on the account provider for authentication of the user
- third parties be able to direct the account provider to initiate the authentication
- the information being exchanged must be encrypted
- authorised sessions be kept as short as possible and terminated upon completion of an action
- the technical specification be documented, and that this be available on request, free of charge, to authorised third party providers, with a summary of the documentation on their website
- account providers ensure that changes to the technical specification are made available to third parties at least three months in advance, except in emergencies
- a testing facility, including support, is made available to authorised third parties
- the level of availability and performance, including support and contingency measures, be the same as the interface made available by the account provider to the user directly
- the data definitions be consistent with ISO 20022
- the information provided be the same as would be available to the user when logging in directly, and
- third parties cannot request information more regularly than four times during a 24-hour period unless the user is actively requesting information.[118]

The main limitation of the EU's approach to technical standards is that it lacks the detail required to provide a standardised approach. The European Banking Authority acknowledges that:

> *When developing these particular RTS, the EBA had to make difficult trade-offs between at times competing demands. For example, the objective of PSD2 to facilitate innovative payment services would suggest that the EBA should pitch the technical standards at a higher, i.e. less detailed level, so as to allow room for the industry to develop industry standards or technical solutions that are compliant with the EBA's Technical Standards but that also allow for innovation over time, to exploit technological advancements and to respond to future security threats. However, this may result in many different industry solutions emerging across the EU, in particular for communication between… [the parties]… This, in turn, could lead to a fragmentation across geographical, sectoral and/or other lines, which would undermine PSD2's objective of integrating retail payments in the EU and facilitating competition across the EU.*[119]

118. The draft RTS also includes rules relating to secure customer authentication, but these relate to banking in general rather than communication with third parties specifically. *See European Commission 2017, 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*. Available at: http://ec.europa.eu/finance/docs/level-2-measures/psd2-rts-2017-7782_en.pdf
119. European Banking Authority 2017, *Final Draft RTS on SCA and CSC under PSD2*. Available at: https://www.eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+(EBA-RTS-2017-02).pdf

A further consequence of this high-level approach to technical standards is that it fails to address the scenarios outlined in the previous section, whereby a bank with legacy systems and limited incentives to embrace Open Banking may choose an unusual interface that would be very difficult for most developers to use.

The UK sets out technical specifications

As EU member nations are able to apply additional requirements on top of the PSD2, the United Kingdom (UK) has chosen to go further and set out a detailed technical specification.

In 2014, the UK Government asked the Open Data Institute (ODI), a not-for-profit organisation co-founded by the inventor of the Web[120] with the goal of improving access to data, to explore how competition in UK banking could be affected by more widespread use of APIs. The report commissioned by the ODI, known as the Fingleton Report,[121] concluded that APIs had significant potential to boost competition and innovation in banking.

In addition to these broader recommendations, the Fingleton Report concluded that it would be important to agree on a common API standard. The rationale for this approach is that a standard API would reduce development costs for the banks as well as third parties.

The Fingleton Report also made a number of technical recommendations. First, the report recommended that the common API standard should use a RESTful architecture, noting some of the technical benefits of a RESTful approach, as well as its popularity among developers. Following this principle of adopting existing web standards, the Fingleton Report also recommended the use of:

- JavaScript Object Notation (JSON) to encode the message
- HTTPS to encrypt the message securely
- a 'battle tested' implementation of OAuth 2.0 for secure authorisation, and
- a sandbox for developers to test their applications.

Following the publication of the Fingleton Report and a call for public responses, the UK Government established the Open Banking Working Group (OBWG) to consider the design of an Open Banking API in detail.

OBWG's considerations were guided by the following principles:

Openness – ensuring accessibility for all interested parties, across a wide range of participants, thereby incentivising adoption, distribution and participation.

Usability – facilitating ease of implementation and a smooth user experience for participants.

Interoperability – promoting and progressing towards an environment where data can be exchanged between parties in a frictionless manner across organisational and technological boundaries.

120. Sir Tim Berners-Lee.
121. Open Data Institute and Fingleton Associates 2014, *Data Sharing and Open Data for Banks: A report for HM Treasury and Cabinet Office*. Available at: http://www.fingletonassociates.com/wp-content/uploads/2014/12/141202_API_Report_FINAL.pdf

Reuse – adopting and leveraging existing standards, taxonomies and data lists wherever possible and practicable to avoid duplicative efforts and maximise interoperability.

Independence – promoting competition among, and avoiding dependencies on, vendor solutions and technologies; preserving optionality in delivery models and implementation technologies.

Extensibility – establishing flexibility and encouraging adoptees to build upon the standard and innovate locally, while providing governance mechanisms to subsequently bring extensions 'back to the core'.

Stability – ensuring the provision of a stable environment for all participants where change is communicated, actioned and governed in a transparent and consistent manner.

Transparency – providing visibility and clarity on issues pertaining to the standard and the environment it operates in (for instance its design, specifications, governance, etc.).

Based on these principles, the OBWG provides an extensive list of recommendations for the technical specification. As per the Fingleton Report, the OBWG recommended using RESTful APIs, with HTTPS for transport, JSON as the message format and the OpenID Connect profile of OAuth 2.0 for authentication.

Other key features of the recommended approach to security included out of band (or multifactor) authentication, and notification of the user out of band (such as over email) when a significant action occurs, such as a new payee being added. These additional security features are particularly important in the UK context because its open banking API is designed to allow write access as well as read access. More generally, the OBWG recommended using a federated approach to identity where all authorised parties mutually recognise the identity assertions made by other authorised parties.

Regarding the standard itself, the OBWG recommended an open license, an established documentation framework, clear versioning rules, including support for major and minor releases, backwards compatibility and adequate notice for third parties of any changes. Similarly, the OBWG recommended that API providers offer a sandbox to developers and meet defined performance indicators for up-time and support.

Technical specifications consistent with the OBWG's recommendations were subsequently published by the Open Banking Implementation Entity (OBIE) in 2017, and will become mandatory for the UK's nine largest banks in January 2018, along with the broader PDS2 requirements. Despite concerns about some aspects of the UK's overall regulatory approach, the technical specifications appear to have broad support in both the FinTech and banking sectors.[122] The technical specification also makes reference to elements of the draft FAPI standard.

122. For example, some parties were concerned that the UK has not provided a framework for clearly assigning liabilities. This issue is addressed in Chapter 4 of this Report.

Australian Open Banking APIs

The technical standards for the Australian transfer mechanism can draw on the approaches used overseas, and in the private sector.

The EU draft RTS on secure communication sets out the minimum functional requirements that would be necessary for a working third party interface for Open Banking. However, the lack of specificity means that the EU does not provide enough detail to produce a standardised approach. Moreover, the lack of specificity provides room for obscure implementations which could impede the Open Banking objective of promoting innovation and competition. The possibility of odd interpretations is particularly concerning since the design of the API would be left to institutions that may not have an incentive to promote competition.

Merely setting out functional requirements may allow for more competition in the design of APIs. However, it would be a barrier to competition in the development of services for end users. Additionally, there will continue to be competition and innovation in the design of APIs more broadly, and this can be incorporated into the Open Banking standard from time to time where appropriate. Providing one or two alternatives to the core API standard is also likely to be cheaper for banks than each developing their own bespoke implementation in the first place.

The lack of specificity in the EU's functional requirements can be partially addressed by reading them together with the design principles developed by the UK's OBWG. An API is much less likely to be poorly implemented if it uses widely adopted existing standards. However, there would continue to be substantial room for different interpretations. For example, the OFX standard could be argued to be the most widely adopted Open Banking standard. However, it is not consistent with current standard practices regarding APIs in general — which is why more modern attempts to develop banking APIs use a RESTful approach.

In summary, the principles of the UK's OBWG and the requirements in the EU's draft RTS on secure communication provide a strong framework for guiding the work of the Australian Data Standards Body, but the Standards themselves need to provide a more detailed technical specification.

Following the EU's functional requirements and the UK OBWG's design principles is likely to lead to something very close to the UK's final technical specification. The UK's specification is in line with widely supported practice for the development of Web APIs, and the approach used to develop open banking APIs in the private sector. A number of submissions to this Review suggest that Australia should draw on the UK's technical standards.[123] Additionally, starting with an existing specification is likely to greatly accelerate the timeline for the implementation of Open Banking in Australia. It may also facilitate international interoperability. For these reasons, the UK's technical specification should be the starting point for an Australian Open Banking standard, with the UK design principles and EU functional requirements providing guidelines for the consideration of the Data Standards Body.

123. See ABA submission, page 9; Raidiam submission, page 3; and FinTech Australia submission, page 5.

Recommendation 5.2 – starting point for the data transfer Standards

The starting point for the Standards for the data transfer mechanism should be the UK Open Banking technical specification. The specification should not be adopted without appropriate consideration, but the onus should be on those who wish to make changes.

There is a long list of possible issues that the Data Standards Body could consider, some of which are outlined below. However, the initial focus should be on finalising the core Standards to enable basic functionality in a way that does not preclude adaptations to deal with other important considerations.

The key design principle for dealing with these additional considerations is *extensibility*, which refers to a system's capacity to be adapted for different purposes. Extensibility does not mean that a system must support as many features as possible immediately. Simple systems that provide limited initial functionality are often more extensible than highly complex systems with a much longer list of initial features.

Extensibility is particularly important in the Australian context because it is likely that in the future a variant of the initial specification will be used for sharing information with third parties in other sectors. For example, it might be used to share energy usage data with third party applications that help consumers manage their power bill. Additionally, while the initial specification will be limited to read access it should not preclude the possibility of providing write access in the future.

The UK's technical specification is well suited to this objective as it was developed with the purpose of allowing write access and is based on standards that are widely used across a range of industries.

Recommendation 5.3 – extensibility

The Data Standards Body should start with the core requirements, but ensure extensibility for future functionality.

It is also important that the Standards not be mandated as the only way of sharing banking information. If parties believe that they have developed a better alternative they should be free to test that option in an open market, provided that Australian law and regulation is complied with. If a significant number of parties choose to use the alternative, then the Data Standards Body should consider whether the alternative can be incorporated into the core Standards.

If the Standards are particularly poorly designed then third parties may continue to prefer to use screenscraping. Given screenscraping is expensive, unreliable and insecure, this should only occur if the Standards are particularly poorly designed as it will almost always be easier to interact with a dedicated interface than to backwards engineer an interface that was intended for another

purpose.[124] This Review does not make any recommendation that the Government should endorse screenscraping. However, banning it would remove an important market-based check on the design of Open Banking.

Additional issues raised through consultation

A number of specific concerns were raised during the consultation process regarding the data transfer mechanism. Using the UK and EU approaches as a starting point addresses many of these issues implicitly. However, some issues warrant explicit consideration.

Secure, customer-friendly authorisation and authentication

The protocol for authorisation and authentication must balance a customer-friendly user experience with security considerations.

The approach set out in the UK specification involves third parties redirecting the user of their application to the user's bank's website so that they can authorise the transfer of information (see Figure 5.2). This approach can be very secure if implemented appropriately and it also supports a smooth customer experience.

However, a redirect model is susceptible to phishing. Phishing involves a bad actor attempting to gain a user's credentials by posing as a trusted party. The redirect flow does not provide a third party with a user's credentials, however, a bad actor may set up a fake third-party website (or take control of a legitimate one) and redirect the user to a fake bank website that steals their details. These details can then be used to login via a legitimate channel to steal information. Phishing mitigation is primarily based on educating users to navigate directly to their bank's website, rather than following links provided on other websites or via email. Consumers are also encouraged to check the address bar of their web browsers to make sure the domain is actually their bank's domain, but this can be difficult as phishing sites use addresses that closely resemble the bank's legitimate address.

Phishing attacks are already mounted against online banking, but sharing information with third parties increases the 'attack surface'. As the number of participants in the market increases, consumers are likely to find it harder to confirm a website's authenticity and may be more likely to follow links to websites rather than navigating to websites directly. Third parties will also have fewer resources than banks to ensure that phishing sites are shut down quickly.

A decoupled model

An alternative to the redirect model is a 'decoupled' model, which makes customers navigate to the data holder's website directly. In this model the third party's authorisation request is passed to the data holder via the user. This may involve the user copying and pasting a code between the data recipient and the data holder, or the code could be passed as a cookie in the user's browser.

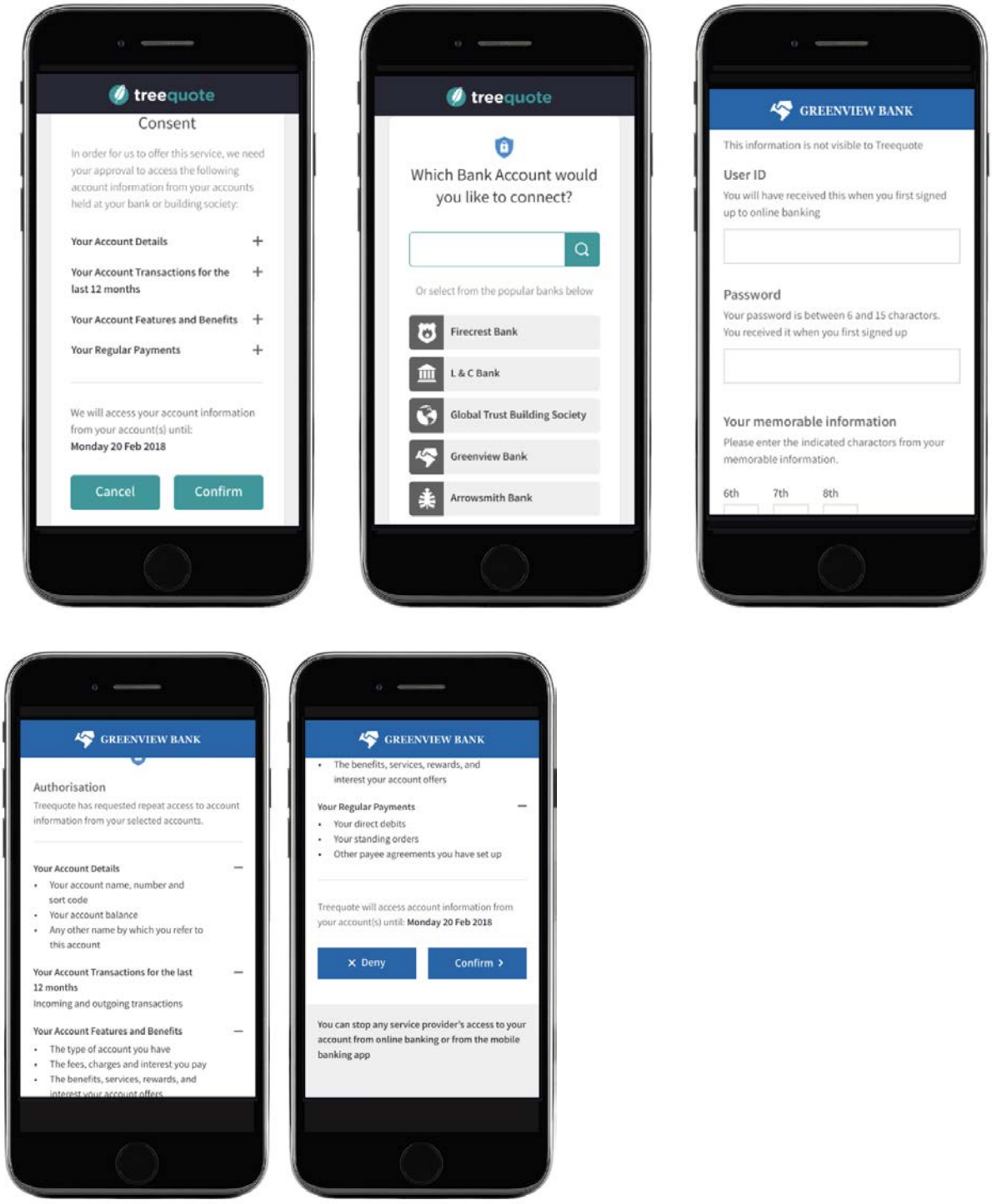
124. Additionally, some third parties may engage in screenscraping to provide payment services until an API with write access is also provided.

Removing the redirect from the authentication flow and requiring the user to navigate to the bank's website makes such attacks less likely. However, it does not eliminate the risk of phishing as a poorly educated user could still be convinced to follow a redirect even if it is not normally part of the authentication process. Requiring users to navigate to bank websites separately also adds friction (that is, customer inconvenience) to the authentication process. The need to copy and paste a code adds a further step and the alternative of using cookies poses its own problems. Other alternatives could also be possible.

Multifactor authentication

Another way to mitigate the risk of phishing and other attacks that may lead to credentials being compromised is to use multifactor authentication. This is already commonly used by many banks to authorise higher risk actions such as adding a new payee. Using multifactor authentication greatly reduces the risk of a bad actor gaining access to a customer's account. However, it does not eliminate the risk entirely as there are also ways that multifactor authentication can be circumvented, and security breaches may still occur if multifactor authentication is not required for all transactions. Multifactor authentication also adds some additional customer friction.

Figure 5.2: UK's Open Banking Consent Model for Account Information



Source: UK OBIE, 2017, Open Banking Consent Model Guidelines

The Data Standards Body should carefully weigh the merits of the redirect and decoupled models. However, the Data Standards Body should take into account that many open banking implementations already use the redirect model. Careful consideration would be needed before pursuing the decoupled approach. The FAPI working group has recently agreed to develop a decoupled approach as an option under the overall specification, but this work has not yet occurred.

Significantly, a decoupled model is different from the model proposed by the ABA where the customer would initiate the process of sharing information with third parties from their bank's website or mobile app.[125] The approach chosen should minimise the ability of the data holder to interpose itself in the relationship between the user and the data recipient.

Recommendation 5.4 – customer-friendly authentication and authorisation

The redirect-based authorisation and authentication flow detailed in the UK technical specification should be the starting point. Consideration should be given to the merits of a decoupled approach provided it minimises customer friction.

Read-only credentials

Another option for reducing the risk associated with Open Banking is to issue read-only credentials. Providing read-only credentials would mean that the risk if a user's information is compromised is limited to the loss of data rather than direct financial losses as a result of money being spent or transferred. However, being forced to remember an additional set of credentials creates an increased burden for the customer, and there is a good chance that customers will use the same password for both. The release of private or commercially valuable information can also cause direct financial loss. Additionally, while transactions can often be reversed information can almost never be reclaimed once it has been released.

Whether it would be appropriate to issue read-only credentials should be investigated through further consultation with interested parties as part of the standards development process.

Additional barriers to authorisation

The Review considered whether banks should be able to restrict a customer's capacity to grant consent to share information with third parties to pre-approved use cases. As noted in Chapter 4, the Review's position is that such restrictions would create unacceptable barriers to innovation and competition. Consumers should be free to provide consent to any third party that is accredited. If a third party is found to be misusing the data that is shared with them, such as by breaching privacy or consumer credit laws, then that issue should be dealt with directly.

Similarly, banks should not put in place unreasonable additional steps that consumers must complete to authorise the sharing of information with a third party. As noted above, multifactor authentication is a reasonable requirement to limit phishing and other security risks. However, the form of multifactor authentication should be consistent with risk management practices applied to direct interactions between the customer and the bank. For example, if multifactor authentication for issuing a payment to a new payee involves entering a second factor sent to the customer via an SMS then it would be unreasonable for banks to require a voice print and face scan to authorise the sharing of information with third parties.

125. See ABA submission, pages 11 to 13.

Recommendation 5.5 – no additional barriers to authorisation

Data holders may not add authorisation requirements beyond those included in the Standards. Requiring multifactor authentication is a reasonable additional security measure, but it must be consistent with the authentication requirements applied in direct interactions between the data holder and its customers.

Persistent authorisation

Customer convenience is a key consideration for this Review. That means that a customer should not have to reauthorise an application each time they want to access information – in other words authorisations should be *persistent* – if this is desired by the customer. Many use cases, such as a personal budgeting app, would be impractical without persistent authorisation because they require data to be updated regularly.

Persistent authorisation is consistent with the OAuth 2.0 framework and most stakeholders implicitly assume that it will be a feature of the system. However, persistent authorisation should not be perpetual, and should not be the default as one-off authorisations are often all that it is required. As noted in Chapter 4 of this Report, third parties should request only the information that is necessary to provide the service and consumers should be able to limit the period of time for which the authorisation will be valid.

Additionally, authorisation tokens should periodically expire even where ongoing access is necessary. Under the EU draft RTS, the maximum expiration period is 90 days. Australia need not follow the EU rule precisely, but the maximum expiration period should be of a similar order of magnitude – it should not be more than six months but nor should it be seven days.

This means that customers will be periodically prompted to renew their authorisation of third party services. While this creates some inconvenience, it is more secure than forcing customers to explicitly revoke access rights when they have decided that they no longer wish to use a service.

In addition to the periodic expiry of tokens, consumers must also be able to revoke authorisation within the third-party service and, as the ABA has recommended, through their bank.[126] Banks could also, at their discretion, notify customers of all parties with whom they are currently sharing information.

Recommendation 5.6 – persistent authorisation

Customers should be able to grant persistent authorisation. They should also be able to limit the authorisation period at their discretion, revoke authorisation through the third-party service or via the data holder and be notified periodically they are still sharing their information. All authorisations should expire after a set period.

126. ABA submission, page 13.

Access to data

As discussed in the Chapter 3, customers should be able to share all the data that would be available to them through normal online banking services. The definitions of individual data items that can be shared should be based on an existing data dictionary.

For international consistency, the best choice is likely to be the schema provided by ISO 20022. However, as the UK's OBIE notes, several modifications are needed to make the schema more developer friendly, cover all necessary banking data items, and cater to an API context.[127]

The initial specification outlined by the UK OBIE allows requests to be filtered by date, but not by any other criteria. Consideration should be given to allowing a broader range of response filters as this allows third parties to limit their requests for information to the scope that they actually need. Additional criteria for filtering might include by payment amount and payee.

The Review considered several models that would limit the information sent to third parties.

One model involved limiting the information third parties can access to summarised or filtered data, such as account balances or the total amount spent in a particular period. However, this will never be sufficient to cover all possible situations. For example, if a third party uses a machine learning algorithm to classify transactions then summary data is insufficient.

Another possible model involves third parties sending blocks of code for banks (or their trusted partners) to run on their own systems. This has numerous problems if it is to be the sole solution. First, running foreign code on a bank's server poses significant security issues. It also means that third party developers will need to write their algorithms in the language which runs on the bank's technology stack. This is likely to differ from bank to bank, unless the Standard also went so far as to specify how banks run their own backend IT (which seems to go beyond what the Standards should cover). Additionally, a company's algorithms may be a core part of their intellectual property. A Standard that requires that third parties share intellectual property with banks, who may be their competitors, is commercially impractical. Finally, the output of the algorithm still needs to be shared with the user, which means the third party will have access to it at some point.

A third possible model is preventing third parties from caching information. Most applications could probably be written so that they do not hold the customer's data long-term. For example, a budgeting app which allows users to classify transactions could record identifiers that allow the customer's classifications to be relinked to each individual transaction every time they start a new session. However, possible does not mean practical. This approach would make third party applications much harder to write, and for many use cases it would put a much larger drain on the backend infrastructure of the bank and the third party.

Discouraging unnecessary caching of data is a sensible security precaution, but as with the issue of persistent authorisation, this should be achieved through customer consents, control and a risk-based accreditation regime.

127. See UK Open Banking Implementation Entity 2017, *Account Transaction API v1.1.0*. Available at: https://www.openbanking.org.uk/read-write-apis/account-transaction-api/v1-1-0/

Recommendation 5.7 – access to rich data

Customers should be able to authorise access to transaction data in full. Data recipients should not be limited to accessing pre-set functions or sending blocks of their own code to run on the system of the bank or its partner or prevented from caching data. However, participants should be free to offer services that provide more limited data to data recipients who have lower levels of accreditation.

Delegation and middleware providers

Intermediaries play a crucial role in financial services and in the economy more broadly. Often, customer-facing third party applications may prefer to receive their data from a middleware provider, such as Yodlee or Plaid, that offers a single API that can be used to access information from a range of different banks. As discussed in Chapter 4, customer-facing applications that receive information from a middleware provider would still require accreditation and liability would be assigned using existing legal principles. Direct accreditation requirements would not extend to other parts of the FinTech 'supply chain', such as providers of cloud storage services. However, accreditation rules may place limits on who accredited third parties may choose as suppliers.

Individuals may also wish to delegate the authority to authorise third party applications to a trusted advisor such as a lawyer or an accountant. To some extent this issue can be handled by the third-party application creating separate roles for clients, who can authorise a bank to share information, and agents, who can access the information once it has been provided to the third party. However, this still forces clients to periodically access an application that they might not otherwise be using to renew the authorisation when it expires or if the agent changes software. Allowing customers to ask their banks to provide the customer's agent with a credential that allows the agent to authorise the sharing of information with third parties would provide a much smoother customer experience. This issue does not necessarily need to be addressed in the Standards, but it should be given consideration to ensure that businesses in particular are able to fully take advantage of their new Open Banking rights.

Recommendation 5.8 – intermediaries

The Standards should allow for delegation of access to intermediaries such as middleware providers.

Access for those without online banking

Some people who do not use online banking may wish to be able to authorise the sharing of information with third parties. For example, a customer may wish to share information with the financial planning software that their financial adviser uses. Where a bank already offers services other than through online banking, it should also be possible for people without online banking to authorise the sharing of information with third parties. This would require bank employees to be given the authority to authorise the sharing of information with a third party at a customer's request.

For example, a customer may ask a teller at a bank branch to authorise the sharing of information following the same procedures currently used to authorise payment.

Recommendation 5.9 – access without online banking

The Standards should allow users who do not use online banking to authorise the sharing of information through service channels which are ordinarily provided by the data holder.

Facilitating real time information access

Some use cases require access to near real-time information. For example, an app which provides a push notification each time a new transaction occurs could let individuals self-monitor credit card fraud. The demand this places on systems raises the question of whether the number of API calls that third parties can make should be restricted. The EU draft RTS addresses this issue by distinguishing between customer-initiated requests and requests initiated by the third party independently. Customer-initiated requests are allowed to be unlimited as they are already unlimited through existing online banking services. However, third party initiated requests are limited to four per day, though this limit can be exceeded with the agreement of the financial institution. No consideration is given to establishing a push API where a third party will be notified if an event (such as a new transaction) occurs.

In the absence of allowing banks to charge for API calls, some form of arbitrary rate limit may be required to reduce unnecessary, frivolous or excessive requests. The EU approach offers a possible compromise, although it may be difficult for banks to tell whether an API call is customer-initiated. In any case, this issue should be explicitly considered by the Data Standards Body, including whether the standard should be amended to allow for push access in the future.

Recommendation 5.10 – access frequency

The Data Standards Body should determine how to limit the number of data requests that can be made.

Transparency

The data transfer mechanism should facilitate transparency.

This means, first, that customers should be able to access information about their own usage history as this provides additional protection against the possibility of unauthorised access. A record of access should be available to the customer through their bank. This information should itself be subject to the Customer Data Right and capable of being shared with third parties.

Secondly, institutions should maintain records regarding the overall performance of their API, including outage data and response times. This data will almost certainly be kept as part of normal business practices, but it is important to be clear on this point so that regulators can ensure that a level playing field is provided to all participants.

Recommendation 5.11 – transparency

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.

Chapter 6: Implementation and beyond

This chapter sets out a number of aspects of the implementation of Open Banking in Australia and outlines some issues that may need to be addressed after the system has commenced operation.

Implementation issues include the estimated timeline for implementation, options for a phased approach, design features to reduce compliance costs to participants, aspects of cost recovery, and the importance of a consumer education programme.

Post-implementation issues include a post-implementation assessment of Open Banking and:

- the potential for future payment initiation (known as 'write' access)
- the emergence of a comprehensive digital identity
- a new data ecosystem to assist in advancing the digital economy
- greater transparency in the value of data, and
- interoperability with different jurisdictions.

The commentary in this chapter has been informed by international developments and in other industry sectors. In particular, the Review has benefitted from observing the progress of Open Banking implementation in the United Kingdom (notwithstanding the important differences in the scope of UK's Open Banking).[128]

Implementation timeline

This chapter makes reference to the 'Commencement Date' in a number of its parts as the benchmark from which other dates and periods are measured. The basis for the determination of the Commencement Date for Open Banking is contained in Recommendation 6.1 and related text.

Submissions varied widely on a realistic timeline for the commencement of Open Banking in Australia for both a staggered introduction of certain data sets as well as the full implementation of all elements of Open Banking.[129]

The Review considered the implementation timeline of Open Banking in the UK which had the following key milestones:[130]

- August 2016 – CMA publishes Banking Remedies
- September 2016 – Open Banking Implementation Entity formed

128. Available at: https://www.openbanking.org.uk/about. A number of submissions, including from the ABA, drew heavily upon the implementation model and timeline in the UK.
129. ABA submission, pages 7-8; FinTech Australia submission, pages 17-18; and ANZ submission, pages 3-4.
130. Available at: https://www.openbanking.org.uk/about/. Stage One: APIs for Branch/ATM, Personal Current Account, Business Current Account, SME Lending; Stage Two: Read/Write APIs.

- March 2017 – Stage One of the CMA Remedies delivered
- January 2018 – Stage Two of the CMA Remedies to be delivered (Read/Write APIs).

While such a timeline is instructive, a number of submissions advocated a shorter timeframe than the UK as a result of our system requiring 'read only' data-sharing, whereas the UK's obligation to comply with the EU's Payment Services Directive 2 also requires 'write access'. Other reasons cited for a more ambitious implementation timetable include that Australia could develop technical standards using UK and EU standards as a starting point, whereas the UK had no template.

Working backwards, in order to undertake the 'Steps to Implementation' set out in the next section, it seems that a relatively ambitious lead time would be around 12 months before the Commencement Date. This 12-month period would not commence until the announcement of a final Government decision on Open Banking. Such a time would be shorter than the UK time frame of an estimated 18 months between the publication of the CMA's Banking Remedies and delivery of Read/Write APIs. A period of 12 months would represent a balance between the period of potentially several years advocated by some banks, and the shorter periods advocated by FinTech Australia. The ACCC should monitor progress towards the Commencement Date and be empowered to adjust the Commencement Date if necessary.

The proposed Commencement Date also takes into account the work undertaken in consultation with industry over a period of time in relation to the broader Consumer Data Right. The Productivity Commission's (PC's) Data Availability and Use Inquiry commenced with release of an Issues Paper in April 2016 and the Government announced its support for the PC's final recommendations for a Consumer Data Right, with Open Banking as the first designated sector, in November 2017.

Recommendation 6.1 – the Open Banking Commencement Date

A period of approximately 12 months between the announcement of a final Government decision on Open Banking and the Commencement Date should be allowed for implementation.

Steps to implementation

The main steps required for the implementation of Open Banking following a final Government decision include the following, as shown in Figure 6.1:

- amendments to existing laws and regulations to:
  - give effect to the proposed regulatory framework including the Consumer Data Right
  - modify privacy protections
  - create the comprehensive liability framework
- determining the roles of the regulators and agencies in Open Banking
- establishment of a Data Standards Body and setting Standards

- settlement and promulgation of Rules
- establishment of an accreditation framework and criteria, and
- IT building and testing by Open Banking participants.

Amendments to existing laws and regulations

Chapter 2 recommends that Open Banking be implemented primarily through amendments to the *Competition and Consumer Act 2010*. Amendments will be needed to set out the overarching objectives of the Consumer Data Right, grant the power to the Treasurer to designate sectors to which the Consumer Data Right will apply, describe what the Rules will cover in that sector, and address other considerations described in Chapter 2.

The Rules will contain parameters for accreditation, oversight of Standards-setting processes and outcomes and enforcement of rights in relation to systemic issues.

Chapter 4 explains how the privacy protections will need to be modified to accommodate the dual regulatory model for complaint handling with respect to privacy matters. Other laws may require amendments to align with the new Consumer Data Right.

Ideally, these amendments should be made as early as possible prior to the Commencement Date, in order to allow the subsequent design of Rules and Standards to occur. However, provided there is sufficient certainty about the core elements of the regulatory framework so that Rules and Standards can be developed in parallel, the legislation might be finalised relatively close to the Commencement Date.

Roles of regulators and agencies

Chapter 2 recommends that Open Banking be supported by a multiple regulator model under which the ACCC, as the lead regulator, will have overall responsibility for the system, as well as primary responsibility for competition and consumer issues and standards-setting. The Office of the Australian Information Commissioner (OAIC) will have primary responsibility for privacy protection. ASIC, APRA and the RBA will be consulted where sector-focussed regulatory input is desirable and may have other responsibilities as necessary.

Ideally, in order to allow the subsequent design of the Rules to occur in a reasonable time, determination of the roles of each of the regulators and agencies should be made 9 months prior to the Commencement Date.

Establishing a Data Standards Body and setting Standards

Chapter 2 recommends that Standards are set through a Data Standards Body which incorporates technical expertise and experience in the standards-setting process, has an independent Chair and writes standards with the close involvement of industry. The Government will appoint the Chair of the Data Standards Body and the primary regulator will work with the Chair to establish governance, process and plans for Standards as recommended in Chapter 2, including the establishment of a Standards working group. Chapter 5 sets out the Standards to be developed by the Data Standards

Body including transfer standards, data standards and security standards. Ideally, the Data Standards Body should be established approximately nine months prior to the Commencement Date.

Settlement and promulgation of Rules

Chapter 2 recommends that the lead regulator, the ACCC, in consultation with the OAIC, ASIC, APRA, the RBA and other relevant regulators, be responsible for determining Rules that specify the expectations to be met in Open Banking and the Consumer Data Right. The Rules will be subject to public consultation, finalised by the ACCC and given effect through Ministerial assent. Ideally, the Rules should be settled approximately six months prior to the Commencement Date.

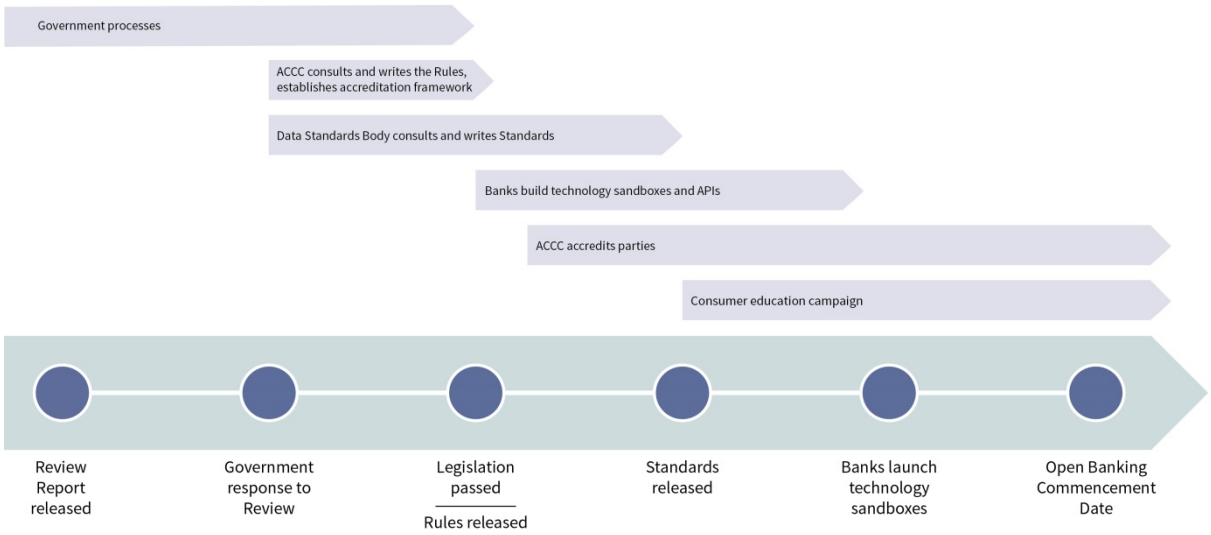
Establishing accreditation framework and criteria

Chapter 2 recommends that the ACCC, in consultation with the OAIC and other relevant regulators be responsible for determining the criteria for accreditation within Open Banking and ensuring the effectiveness of the accreditation process including setting governance standards for the process of accreditation. Ideally, the accreditation framework and criteria should be established approximately six months prior to the Commencement Date.

IT build and testing by Open Banking participants

A period of IT build time and testing by participants in Open Banking will be required. It is expected that, in the 6 months prior to the Commencement Date, early-adopting FinTech firms and the major banks will be actively testing the technology.

Figure 6.1: Implementation timeline



A phased approach to implementation

Many submissions argued for a phased introduction of some type, whether based on type of data holder, type of customer, or category of data.[131] These options are considered below.

Phasing based on type of data holder

A number of submissions supported starting only with a subset of larger firms as data holders.[132] The reasons provided in support of this approach were to ensure timely implementation, minimise the burden on industry, build customer trust and learn from the initial operation of Open Banking in other jurisdictions.[133]

Starting Open Banking with the four major Authorised Deposit-taking Institutions (ADIs) in Australia (the 'major banks') seems logical as together they hold 77 per cent of the Australian personal deposits market.[134] One submission that supported starting with only the major banks pointed out significant resource constraints for smaller banks and argued that only the major banks need be forced into Open Banking, as others will be compelled to join to remain competitive.[135]

The Review acknowledges these potential resource constraints and competing demands for the smaller ADIs to prepare for the implementation of an Open Banking framework. However, customers of those smaller ADIs should not be denied access to Open Banking indefinitely, or even unduly. For this reason, Recommendation 3.8 proposed that the data-sharing obligation on data holders be phased in, beginning with the largest ADIs.[136]

While it is difficult to assess accurately how much time will be required for smaller ADIs to prepare, given the Commencement Date is likely to be no earlier than 12 months from a final Government decision (for practical reasons explained above), the Review does not expect that more than a further 12 months will be required. If more time is necessary, the ACCC should be authorised to defer the Commencement Date for smaller ADIs. Any 'early adopters' could, of course, participate voluntarily in advance of that date.

Recommendation 6.2 – phased commencement for entities

From the Commencement Date, the four major Australian banks should be obliged to comply with a direction to share data under Open Banking. The remaining Authorised Deposit-taking Institutions should be obliged to share data from 12 months after the Commencement Date, unless the ACCC determines that a later date is more appropriate.

131. In this context, a *phased* introduction means staggering the commencement dates for parts of Open Banking or some of its participants.
132. COBA submission, page 14; and ANZ submission, page 4
133. ASIC submission, pages 11, 27.
134. Reserve Bank of Australia – Competition in the Australian Financial System – Public Inquiry, Submission to the Productivity Commission Inquiry, September 2017; referred to in the COBA submission, page 5.
135. COBA submission, pages 5, 9.
136. See Chapter 3.

Phasing based on type of customer

Chapter 3 considered which customers should benefit from the Consumer Data Right, finding that the need for Open Banking was strongest for individuals and small businesses. However, it was concluded that it might be harder to *exclude* large businesses than *include* them, especially given the potential complexity of developing the definition of businesses outside scope. This conclusion was supported by the less complex nature of the transaction data accounts named in Chapter 3 that larger businesses were less likely to hold. Consequently, Recommendation 3.7 proposed that the obligation to share data at a customer's direction should apply for all customers holding a relevant account in Australia. Accordingly, no phasing by customer type should be required.

Phasing based on type of data

Chapter 3 proposed that the categories of data types (data sets) subject to data-sharing obligations should be *customer-provided data*, *transaction data* and *product data*. This section considers the appropriateness of phased commencement dates for different data sets.

The Open Banking regime in the UK adopted a two-stage process of implementation based on data sets.[137] The first stage required sharing of 'reference data' such as branch and automatic teller machine location and certain product information. Feedback from participants in the UK suggests that implementing the initial phase has not achieved significant customer benefits, and the Review therefore believes it is not necessary for Australia to follow that approach.

The second stage in the UK requires the sharing of transaction data and provision of payment initiation services which enables customers to consent to allowing third parties to initiate payments from a customer's account on the customer's behalf. Payment initiation is also known as 'write access' and is discussed later in this chapter, although as noted in Chapter 1, write access is not part of the initial scope of Open Banking in Australia.

While the submissions of both the ABA and ANZ supported a two-staged approach similar to the UK, the ABA proposed the sharing of product and service attribute data in the first phase and customer data in the second phase, whereas ANZ proposed the sharing of product attribute data and transaction data in summarised form in the first phase, and economy-wide open data in the second phase.[138]

The submission of FinTech Australia provided an alternative phasing approach, driven by use cases, commencing with Know-Your-Customer reliance data in the first phase and full read and write access in the last phase.[139] The submissions also provided timeframes for each phase, such as the ABA's support for general product data-sharing within 12 months of certain criteria being satisfied.[140]

137. Available at: https://www.openbanking.org.uk/about/
138. ABA submission, pages 7-8; and ANZ submission, page 3.
139. FinTech Australia submission, pages 17-18.
140. ABA submission, page 7.

Another proposal was to commence with sharing simpler, lower-risk data sets and add higher-risk data sets later.[141] This would allow time to develop:

- a regulatory framework which adequately addresses issues relating to security, liability and privacy of sharing certain data sets, and
- the standards required to streamline the transfer of different types of data sets.

However, provided the earlier recommendations of this Report are adopted, these concerns should have been addressed well before the Commencement Date. In addition, work on developing the Standards will benefit from drawing upon the current data-sharing initiatives in other jurisdictions as well as Australia, including the recent launch by Macquarie of its own Open Banking platform which allows customers to direct the secure transfer of their data to approved third party participants.[142]

A further reason given for a phased introduction for certain data sets is to prioritise certain data sets over others. As described in Chapter 3, the data sets that will be most useful to individual customers are transaction data and product data because they will enable product development and comparisons. The sharing of transaction data will also provide a secure alternative to the current practice of using screenscraping technology to access transaction data from customer bank accounts.

One issue affecting the timing of commencement of transaction data sets is the availability of historical data. As described in Chapter 3, the Review recognises that a requirement to provide seven years of digital transaction data may impose significant costs on data holders particularly if such data is not currently stored in an electronic form and that, therefore, transitional arrangements may be required. Feedback from banks and FinTech firms differed considerably on the point of how much historical data should be made available at the commencement of Open Banking. While FinTech firms made good arguments for 'the more historical data the better', the banks suggested that providing historical data could be problematic. Some historical data is essential for Open Banking to achieve its objectives, but requiring too much too soon may put data holders under unnecessary pressure to upgrade legacy IT systems. The Review has come to the view that an appropriate balance would be that historical data relating to transactions from 1 January 2017 should be included in Open Banking. However, when historical data is of an age that the data holder is no longer required to retain it for regulatory purposes then it should no longer be required to be transferred under Open Banking.

Chapter 3 also recommended including customer-provided data in the scope of Open Banking. As outlined in that chapter, due to pending reforms to Anti-Money Laundering (AML) laws relating to reliance on identity verification assessments performed by other reporting entities, the Review is not in a position to specify the timing for implementation of the customer-provided data sets. The Review notes that timing should be determined by the ACCC once consideration of proposed reforms to the AML laws have been finalised, given that information supporting identity verification assessments is likely to form a large part of customer-provided data.[143]

141. Regional Australia Bank submission, page 1.
142. Available at: https://www.macquarie.com/au/business-banking/business-strategy/expertise/what-the-new-wave-of-technology-means-for-you
143. See Recommendation 3.4.

Accordingly, transaction data and product data will likely be in scope before customer-provided data, but as a consequence of the timing of the AML reforms, rather than due to an intentional phasing.

Recommendation 6.3 – commencement date for data

From the Commencement Date, Open Banking should apply to transaction data and product data. However, Open Banking should not apply to transaction data relating to transactions before 1 January 2017. Open Banking should apply to customer-provided data and the outcomes of identity verification assessments on a date to be determined by the ACCC.

Consumer awareness and education

Why do we need consumer education?

The role of consumer awareness and education is to equip the public with knowledge for making decisions relevant to their everyday life in a consumer society. While Open Banking is a simple concept – giving customers the ability to instruct the secure sharing of their banking data and to unlock its value – there are a number of complex aspects.

One submission considered that a lack of understanding by customers would undermine efforts to introduce an effective data-sharing framework, and referred to research in the UK in October 2016 which found that 90 per cent of adults had never heard of Open Banking.[144] The ABA's submission viewed customer education as a 'key component to ensure the benefits of open data are realised across the economy', and argued that an understanding of the opportunities and implications of an open data environment is critical.[145] FinTech Australia's submission regarded a nationwide communication and education campaign as a vital component of any open financial data framework in Australia.[146]

At the roundtable for consumer advocates conducted by the Review, participants made it clear that a consumer centric outcome for Open Banking would require effective consumer education on the benefits and risks as well as responsibilities arising from participation.

Consumer education opportunities in Open Banking

Open Banking will inspire customers' confidence if they have an understanding of:

- their rights and responsibilities
- the value of their data, and
- the risks in the system and the safeguards to minimise those risks.

144. CBA submission, page 7. Refers to Equifax/YouGov, 'Use of Personal Data', October 2016, Available at: https://www.equifax.com/assets/unitedkingdom/yougov_survey_use_of_personal_data.pdf
145. ABA submission, page 3.
146. FinTech Australia submission, page 38.

One submission considered that consumer education should go further than providing information to customers and also seek to 'build enthusiasm and momentum to encourage customer take-up of the data opportunity'.[147]

A consumer advocacy group joint submission highlighted that financial literacy will play an important role in empowering customers participation in Open Banking.[148] ASIC coordinates the Government's financial literacy programmes under the National Financial Literacy Strategy.[149] The Strategy provides a framework to guide and co-ordinate financial literacy initiatives of key stakeholders across the business, community, education and government sectors. One initiative is ASIC's *MoneySmart* website which provides free and impartial financial information on topics such as managing money and borrowing and credit. ASIC's *MoneySmart* website or a website specific to Open Banking managed by the ACCC is a potential tool with which to reach and educate consumers on Open Banking.

A number of financial institutions that already provide data-sharing services have consumer education activities in place. Acknowledging the importance of such activities, one submission recommended that 'resources be focussed on a comprehensive education programme across the banking sector aimed at ensuring consumers have resources and support in relation to Open Banking'.[150]

Public events such as conferences in relation to Open Banking developments are also opportunities to raise awareness. Australian Payments Council held an industry hackathon during 2017 to 'generate awareness around the value of data, focusing on positive consumer outcomes' for participants in Open Banking. The event involved the collaboration of over 120 developers, designers and innovative thinkers from four states across Australia.[151] In addition to targeted consumer education programmes, such events are an effective means of raising awareness across a broad spectrum of market players and potentially industry and consumer groups.

What timing is most effective for consumer education?

A number of submissions highlighted that consumer outcomes and consumer education is vitally important both in supporting the initial launch of the reforms and the ongoing management of customer expectations.[152]

In considering whether a programme of consumer education at an early stage is important for customers, the Review considered an assessment by the UK Financial Conduct Authority (FCA) of the impact of some of the early measures implemented in UK Open Banking on consumer banking behaviour which showed the benefits of consumers receiving information 'just in time'.[153]

147. FinTech Australia submission, page 38.
148. Consumer Action Law Centre, Financial Rights Legal Centre, Financial Counselling Australia submission, October 2017, page 8.
149. Available at: http://www.financialliteracy.gov.au/. Public consultation paper on the Strategy released by ASIC in October 2017
150. CBA submission, page 7.
151. Australian Payments Council submission, page 6.
152. Australian Payments Council submission, page 6; and CBA submission, page 7.
153. FCA, *Message received? The impact of annual summaries, test alerts and mobile apps on consumer banking behaviour, Occasional Paper No. 10, March 2015*. Referred to in ASIC submission, page 10.

There will be some potentially key points in the implementation timeline where consumer education opportunities arise:

- at the time of the announcement by the Government of this Report
- during public consultation by the ACCC on the Rules
- at the time of the announcement by the ACCC of the establishment of the Standards
- in the immediate lead up to and at the Commencement Date, and
- during the first year of operation of Open Banking in Australia.

Who should provide consumer education?

Submissions from industry associations including the ABA and FinTech Australia held the view that Government, industry and consumer groups all have a role to play in customer education.[154]

In relation to the Government's role, the PC Data Report recommended that the ACCC as lead regulator with respect to the Consumer Data Right be resourced to conduct consumer education.[155] As the proposed lead regulator, the ACCC would be the appropriate body, in consultation with the OAIC, to develop a consumer education programme for Open Banking.

Submissions noted that a certain amount of consumer education and awareness activities are already being undertaken by banks as well as FinTech firms and industry groups in relation to current data-sharing practices as well as the development of Open Banking.[156]

Limitations of consumer education

A number of submissions raised the issue that consumer behavioural research in recent years has exposed the limitations of consumer education and disclosure regimes and the impact on the effective implementation of policy measures.[157] Consumer behavioural factors, including how and when information is presented, can either improve or impede good consumer outcomes.[158]

One submission proposed consumer testing and collecting and analysing relevant data to measure outcomes in order to avoid relying on assumptions about how consumers and firms will behave in response to the introduction of Open Banking.[159] A post-implementation assessment, as described in the following section, would provide an opportunity to conduct such testing to examine the adequacy of regulatory powers to deliver effective and customer centric Open Banking.

---

154. ABA submission, page 3; and FinTech Australia submission, page 38.
155. PC Data Report, Recommendation 5.4, page 37.
156. CBA submission, page 7.
157. Consumer Action Law Centre, Financial Rights Legal Centre, Financial Counselling Australia submission, October 2017, page 8.
158. The relevance of recent social and behavioural science developments is described as follows: Through decades of empirical research and testing, these insights have added to traditional economic models, which are often based on assumptions about how an average person should behave. Behavioural sciences are increasingly being applied in a government policy-making context, as well as in private industries. Insights from the behavioural sciences are relevant because they identify factors that can prevent more informed decision making by consumers. ASIC submission, page 31.
159. ASIC submission, page 10.

Recommendation 6.4 – consumer education programme

The ACCC as lead regulator should coordinate 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.

Costs of implementation

Regulatory costs

Chapter 2 set out the roles of the regulators in supporting the Open Banking regulatory framework. The ACCC will be the lead regulator, with primary responsibility for competition and consumer issues including accreditation of participants and standards-setting. The OAIC will be primarily responsible for privacy protection. Other relevant regulators, including ASIC, APRA and the RBA, will have a support and consultation role.

Whenever the need for activities by regulators arises, there is a fundamental question as to how those activities should be funded. Current Government policy is to recover the costs of regulatory activities directly from industry participants in a number of cases. The Government's Charging Framework states that 'where appropriate, non-government recipients of specific Government activities should be charged some or all of the costs of these activities'.[160]

Cost recovery in accordance with this policy can occur in one of two ways. First, where there is a direct link between the entity creating the need for a regulatory activity and the beneficiary, the variable costs created by that entity could be recovered by way of fees for services. Secondly, where the amount of effort a regulator exerts in regulating each entity is approximately equal across a sector, costs may be recovered by way of industry levies.

In Open Banking, the costs of accreditation in particular would be susceptible in theory to 'fee for service' charging on the basis that the costs would vary with the standards and therefore the risks of the entity seeking accreditation. However, given ADIs will be given automatic accreditation, such an approach would create a distinct barrier to entry for non-ADIs, contrary to the spirit of the measure (and go against the PC's advice).

Similarly, an industry levy may serve this function when the size of the industry is relatively stable and the system relatively mature. However, Open Banking is the first step in a broader Consumer Data Right and it would be unfair to apply all the establishment costs to just the first sector. The number of initial participants in Open Banking is expected to be small, with a phased introduction commencing with only the four major banks plus other early adopters. Starting cost recovery with a very small pool would load the costs on to the early participants.

160. Available at: https://www.finance.gov.au/resource-management/charging-framework/

There is also an argument that cost recovery through an industry levy is not appropriate where the regulation is being imposed for the benefit of a third group (such as the general banking public) as is the case with Open Banking. Otherwise, the cost recovery is merely a very narrowly-based (and therefore economically inefficient) form of taxation.

For these reasons, at this early stage, the Review considers that it would be difficult to impose either a fee for service or an industry-funded model. As Open Banking will form part of the broader Consumer Data Right that will benefit the general public, it is appropriate that the regulatory costs are funded from general taxation revenue at the outset. The initial funding arrangement could be re-considered after a period of operation of the Consumer Data Right, when there is a more certain number of participants and established cost structure. The Review proposes that review of funding should form part of the post-implementation assessment discussed later in this chapter.

Regulatory compliance costs for industry and participants

A number of submissions sought to identify different types of costs for industry and participants in the implementation of Open Banking. Submissions showed a significant variation in estimated costs. At the same time, there was acknowledgement that 'careful planning will allow the Government and industry to jointly achieve the outlined objectives while minimising associated costs'.[161]

The UK Report on Data Sharing and Open Data for Banks, published by the Open Data Institute and Fingleton Associates in 2014 (the Fingleton Report), considered different cost aspects of establishing an Open Banking system following consultations with a number of organisations.[162] The Fingleton Report described the importance of non-tech costs (such as internal decision-making on technologies, legal requirements, data security and privacy standards), cost implications of APIs compared with manual file downloads, the challenges of working with legacy banking IT systems and the necessity of skills and capabilities.

The submission of NAB outlined that the key costs in implementing Open Banking would be (i) identifying, collating, verifying and aggregating the data, (ii) developing technology systems and infrastructure to complete such work, and (iii) ongoing costs of data reporting and system maintenance.[163] The submission also pointed out that cost estimation is difficult until details of the approach, data format and commencement date are settled.

The submission of the Customer Owned Banking Association referred to the PC Data Report and costs of building the technical infrastructure required for the transmission of data to a third party. In addition, the submission referred to upfront costs to implement internal processes, compliance and legislative obligations and ongoing operational costs including subscription charges for infrastructure and platform licensing.[164]

161. CBA submission, page 9.
162. Open Data Institute and Fingleton Associates 2014, *Data Sharing and Open Data for Banks: A report for HM Treasury and Cabinet Office*. Available at: http://www.fingletonassociates.com/wp-content/uploads/2014/12/141202_API_Report_FINAL.pdf
163. NAB submission, page 17.
164. COBA submission, page 9.

The submission of CBA drew upon research in the UK and provided a table showing a comprehensive breakdown of UK Open Banking direct implementation costs listed below.[165] The submission acknowledged that the scope and technical complexity of the UK model and the maturity and complexity of existing systems of the nine banks subject to Open Banking in the UK impacted on the estimates of:

- technology costs including system build and integration
- business costs including change management, risk and regulation
- industry costs including administration of the Open Banking Implementation Entity and the development and maintenance of standards, and
- indirect costs including change impacts, servicing and supporting customers.

Design choices to minimise implementation costs

There are a number of practical design choices in creating Open Banking that can moderate both execution risk and potential financial burdens.[166] These include removing uncertainties, reducing costly barriers to entry for smaller players and enabling cost-sharing opportunities.

Removing uncertainties

Market participants provided feedback to the Fingleton Report that a lack of certainty in relation to technologies, legal requirements and data security and standards would have the potential to increase implementation costs considerably.[167] Providing such certainty has been a key driver to the following proposals of the Review, leading to recommendations to:

- establish a governance framework for setting Standards relating to technology and security (see Chapters 2, 4 and 5)
- clarify the scope of data and participants and the legal obligations arising from the proposed Consumer Data Right (see Chapter 3 and 4)
- confirm existing and new safeguards to be established to protect consumers (see Chapter 4), and
- clarify that Open Banking will not include payment initiation (write access) at commencement (see Chapter 1).

Reducing costly barriers to entry for smaller players

A number of smaller FinTech firms and representatives for smaller ADIs raised concerns in submissions that regulatory requirements could result in significant costs relative to size of the entities.[168] Compliance with such regulation could become 'a burdensome and unintended tax on innovation' and deter the establishment of sustainable business models in the Australian market.[169]

165. CBA submission, page 9.
166. CBA submission, page 10.
167. Fingleton Report, page 84.
168. COBA submission, page 9.
169. MoneyTree submission, page 3.

With a focus on ensuring the benefits of competition and innovation can be realised, the Review sought to accommodate such concerns in the recommendations to phase commencement of Open Banking (refer to earlier in this chapter) and establish a tiered accreditation and registration framework to reflect the intended use and risk of the data held by a third party (refer to Chapter 2).

Enabling cost-sharing

Frameworks that allow for cost-sharing, such as the cost of assessing third party data recipients seeking to participate in the Open Banking system, can be an effective way to reduce implementation costs.[170] The Review has sought to leverage such opportunities by recommending:

- the establishment of an accreditation framework supervised by the regulator, following consultation with other relevant regulators and industry (see Chapter 2)
- the establishment of a Data Standards Body supervised by the regulator to set Standards incorporating expertise as well as industry and consumer experience (see Chapter 2)
- that data holders that are ADIs automatically satisfy the accreditation criteria (see Chapter 2), and
- that participants in Open Banking be allowed to rely on identity verification assessments of other participants if the AML reforms relating to reliance proceed (see Chapter 3).

Recommendation 6.5 – the appropriate funding model

As banking is the first sector to which a much broader Consumer Data Right will apply, it would be difficult to impose an industry-funded model to cover regulatory costs at the outset. Neither the total costs, nor the number of sectors or participants will be known for some time, so it would be impossible to make an estimate of the average cost until the system is well-established. The funding arrangement could be reconsidered after a period of operation, when there is a more refined cost structure and greater certainty over the number of participants.

Post-implementation assessment

While it is expected that Open Banking will deliver major benefits, all regulatory reforms are essentially propositions to be tested and should therefore be evaluated for their effectiveness.

To assess Open Banking, benchmarks and indicators to show changes in competition will need to be developed. While account switching has sometimes been considered as an indicator of competition between banks in the past, it is unlikely to be a robust indicator of competition, or of measuring the effectiveness of Open Banking reforms to increase competition. This is because there are significant other reasons why a customer may not want to switch accounts, for example the customer may value the convenience of having accounts co-located at the same bank more than the benefits from

170. Fingleton Report, page 84.

an alternative bank product or the customer may be able to achieve better conditions on their account though discussion with their bank without switching.

An evaluation of Open Banking reasonably soon after implementation would also provide an opportunity for an assessment of the need for any changes to make Open Banking more effective and minimise the effects of any unintended consequences. It would also be beneficial to examine how Open Banking aligns with the broader Consumer Data Right regulatory structure as it is applied to other sectors of the economy.

The post-implementation assessment should provide sufficient time for customers, FinTech firms, banks and other players to change their behaviour as a result of the reforms. While we can expect FinTech firms to move quickly, banking customers have historically had a reticence to change behaviour, with some customers staying with the same bank where they opened their first account for their entire life. While Open Banking will make it easier for customers to change accounts, it is expected that customers will take some time to change their mindset. Consumer education will help in providing awareness of the benefits of Open Banking and FinTech firms are expected to be active in encouraging customer uptake.

The Review has concluded that an evaluation of the effectiveness of Open Banking be undertaken 12 months after Open Banking commences. While the review will occur before the smaller banks are obliged to provide access to data, this will provide sufficient time for the major behavioural response of the reforms to be observed. The timing will also enable the assessment to draw on the experience of participants in the UK's open banking reforms that are already underway.

The assessment could be undertaken by an expert lead with secretariat support from a government agency. It is also proposed that the review engage with those involved in Open Banking and interested parties such as consumer advocate groups.

Recommendation 6.6 – timely post-implementation assessment

A post-implementation assessment of Open Banking should be conducted by the regulator (or an independent person) approximately 12 months after the Commencement Date and report to the Minister with recommendations.

Beyond Open Banking

This Review has been conducted at a time of major international reforms in the banking and payments sectors. These are most notably Open Banking in the UK and the revised Payment Services Directive (PSD2) and General Data Protection Regulation (GDPR) reforms in Europe. Domestically there are also reforms being progressed through the National Innovation and Science Agenda outside of the banking sector that promote innovation and enable greater access to government-held data.

While some of these reforms are broader than Open Banking, they indicate where further benefits for customers may be unlocked and greater competition in financial services can be achieved.

Potential for future write access

The Terms of Reference for this Review focus on data-sharing between parties, known as read access. This approach differs from the UK Open Banking reforms which implement both read and write access reforms. Write access allows third parties to be able to make payments from a customer's account on the customer's behalf. The EU's PSD2 reforms also enable write access for payment initiation service providers. These reforms acknowledge the popularity of internet and mobile banking and will enable banking using these methods easier.

Write access creates further opportunity for FinTech and other businesses to create innovative services. The type of services brought by this opportunity will evolve over time, but it is easy to imagine services that make it more convenient for a customer to manage their finances, meet payment obligations, or increase their ability to achieve better return on their funds.

Box 6.1: Write access under the EU's PSD2

Write access envisaged under PSD2 enables people, including merchants, to use a preferred payment service provider to process their payments. A preferred payment service provider is likely to be the one that has lower fees or provides additional services that the customer values. The payment service will not have to be offered by the customer's own bank. This is in contrast to the current situation where the customer's bank has a payment service, such as MasterCard or Visa, connected to an account.

Under PSD2 a customer will be able to make an online purchase without needing to be referred from a merchant's website to an intermediary's portal to make the payment or go to their own bank's website to enter the merchant's details. Instead, customers will be able use the merchant's direct online banking portal to make the payment. Merchants will be able to connect directly to the customer's bank account using an application programming interface (API) without intermediaries in the process.

While many merchants appear to provide this type of direct payment service the current service requires the involvement of a number of intermediaries. Currently businesses must use an electronic payment provider intermediary who then contacts the customer's credit card company to charge the customer's bank account.

PSD2 should lead to lower payment services fees for the merchant that either add to the profits of the merchant or get passed onto customers through lower costs. It is also envisaged that payment functionality would be built into large websites such as large social networking sites where users would be able to make payments direct to friends through their social networking site identity and without the need to know their friends' bank details.

Some submissions claim that the biggest reform to empower customers and improve bank competition is to enable customers to provide third party write access.[171] Proponents of enabling write access point to the benefits of a greater range of services that people can use to better manage their finances or make payments with less hassle. They argue that, due to the increase in the number and variety of new services that will emerge, the cost of services will fall and believe sufficient security procedures will manage the risk of malicious activity.

There is some demand already for write access services that can be seen by the growth of screenscraper businesses that offer write access services to customers. Unlike the current conditions under which screenscrapers operate, where there are untested regulatory protections for their customers, creating a write access would provide a regulatory framework that entrenches operating requirements and customer protections.

171. FinTech Australia submission, page 5; and Cuscal submission, page 4.

Other submissions have highlighted risks of implementing write access.[172] These submissions argue that write access creates major security risks for customers. If a customer's account was illegally accessed, the malicious party could impersonate the customer in addition to being able to transfer money to steal it or to enhance the creation of a false identity. Write access could give malicious actors a greater incentive to make cyber-attacks because the party with write access would be a more lucrative target.

The recommendations in this Review could result in a fundamental improvement in the power that bank customers have and how banking services are utilised in Australia. For Open Banking to succeed customers need a high level of confidence that their data is secure and that it is only being used for the purpose that consent is given. If write access was created before Open Banking was fully bedded down, that may put its success at risk. Further, while write access has significant benefits, it may take some time for customers to feel comfortable with third parties acting on their behalf. In addition, the New Payment Platform (or NPP) — scheduled to be available to consumers by February 2018 — will enable real time person-to-person payments in addition to more data being able to be included in payment information. Although write access is beyond the Terms of Reference of this Review, for these reasons it would be premature to consider implementing it at this stage.

An assessment of the success of the 'read access' Open Banking reforms should be undertaken before any consideration of moving to write access reforms is made. Part of that assessment should be an analysis of the growth in customers' use of the current providers of write access services via screenscraping. Customer experience and take up of real time person-to-person payments using the NPP infrastructure should also be taken into account in considering implementing write access.

The emerging comprehensive digital identity

The connection between Open Banking and a framework for digital identity has been made in a number of submissions.[173]

The development of a digital identity strategy was a recommendation of the Financial System Inquiry.[174] A digital identity is a verified identity that enables a person to prove who they are in a digital environment and it is a means for customers to verify their identity that would make opening a new bank account easier. As has been noted by the RBA:

> *A framework for trusted digital identity is a related initiative that has the potential to make online interactions more convenient and secure, including in the context of open banking. A trusted digital identity could help mitigate the scope for identity fraud, while providing convenient authentication, as part of an open banking regime.*[175]

172. Westpac submission, page 4.
173. RBA submission, page 4; ANZ submission, page 11; CBA submission, Part B pages 7-8; and FinTech Australia submission, pages 30-31.
174. Recommendation 15.
175. RBA submission, page 4.

It has been submitted that the more cumbersome it is for customers to change bank accounts the less likely they will be to move to a more suitable banking product.[176] Cumbersome processes in qualifying for and opening a new account will hamper achieving the benefits of Open Banking.

One process that creates friction is the identity verification process that potential customers must undergo before they can open an account at a new bank.[177] Identity verification assessments required under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) are an integral part of minimising the risk of money laundering and terrorism financing. However, the documentation that customers must provide to satisfy them can be burdensome and time consuming, creating a disincentive for people to open new accounts.

The Review has recommended that, if consistent with proposed changes to the AML/CTF Act, the outcome of an identity verification assessment should be able to be relied upon by another entity (Recommendation 3.4).[178] If implemented, this recommendation should create an authentication framework which could then be used with banking service providers. This should remove the need for the customer's new provider to undertake its own identity verification check of the customer, saving time and effort for the customer and removing a significant disincentive to access new banking services. It would also make the assessment process easier for the new provider. This could be seen as an indicator of the potential benefits of the development of a customer-driven re-useable digital identity in Australia.[179]

The Digital Transformation Agency (DTA), in conjunction with a number of other government agencies,[180] has been developing a voluntary digital identity service (Govpass) as a stream of the National Innovation and Science Agenda. The service offered by Govpass will complement the Australian Government's Document Verification Service that government agencies and private sector businesses commonly use to verify the authenticity of government-issued documentation such as passports, visas and birth certificates.

Govpass will be an online service that people can use to establish a digital identity that they can then use to verify their identity with Government agencies, for example with the ATO when applying for a tax file number. Govpass will also be able to be used by private sector businesses wanting to verify a person's identity.[181] The DTA expects to be testing Govpass with a limited number of Government agencies by 2018.

176. FinTech Australia submission, page 26.
177. Another reason is that some people are reluctant to open a new account to replace an existing one because they think it is too difficult to move all of their recurring debit and credit payments from their existing account to a new account. Open Banking could assist in streamlining this process as well.
178. The 2016 statutory review of the AML/CTF Act recognised that the ability to rely on the identification of another party would be an important reform that could deliver greater efficiencies and significant regulatory relief for reporting entities under the AML/CTF regime.
179. ANZ submitted that the KYC use case could not be properly met with Open Banking and that the Government may like to consider digital identity as an alternative solution for this issue. ANZ submission, page 11.
180. Australia Post and the Departments of Immigration and Border Protection, Human Services, Industry Innovation and Science, the Australian Taxation Office (ATO) and the Attorney-General's Department.
181. The business must have the consent of the customer before it can verify the customer's identity using the Govpass service.

Private sector work on digital identity is also taking place in Australia and the involvement of the private sector in Australia's digital identity framework was encouraged in some submissions.[182]

Success in the work on digital identity in Australia will have substantial benefits for the effectiveness of Open Banking. The Review sees strong merit in this work continuing and the development of an Open Banking system that has the flexibility to incorporate future developments in digital identity in Australia.

A new data ecosystem to advance the digital economy

As Open Banking progresses it should connect more customers, data holders and data recipients. All of these would be linked by their participation in a system which has shared rules and standards under which customer data and new and existing services and products are provided and exchanged. The foundation of the system is customers, as they will have relationships with both data holders and data recipients. However, this connection should be strengthened by some participants performing more than one role, for example by being both a data holder and a data recipient, or perhaps even a customer as well.[183] The connections should increase as other sectors are added to the Consumer Data Right.

As the connections increase and participants come to rely on the customer-directed flow of data between them, a data ecosystem should emerge. The increasing use of data, in a secure ecosystem with a strong governance structure, could be tremendously beneficial. From a customer perspective, the ability to provide their data that is held by one service provider (like a bank) to another in a completely different sector (like a telecommunications provider) could enable an entirely new field of products and services to be offered, enhancing choice and convenience. For data holders and recipients, this new potential source of information enables better services to be offered, and a more precise product design to meet customer needs. The more successful the ecosystem is, the more the participants will grow to rely on it. This is already shown in other important systems, like our payment systems, clearing systems and markets used for finance, energy and risk.[184]

As noted throughout this Report, it is important that Open Banking as a system is sustainable. Part of this is ensuring that the risks in such an ecosystem are managed. The risks are not limited to the impact on particular customers and they extend to the impact on the system itself. The liquidity in the flow of data becomes important when participants in the ecosystem are relying on it in order for their businesses to function. For example, if there were to be a significant data breach by a data holder then not only could there be an impact on that data holder's customers, but there could be a loss of confidence in the system as a whole, which would affect other participants as well.

Accordingly, it is important that in the future, the regulatory framework enables consideration of issues from a systemic stability perspective as well as from a customer perspective and a competition

182. Digital identity work is mentioned in the Australian Payment Council submission, page 7 and CBA submission, page 8. A request for caution in implementing a solely Government-built and controlled approach was contained in the FinTech Australia submission, page 31. Involvement of the private sector also formed part of the recommendation on digital identity in the Financial System Inquiry.
183. Data holders may also be data recipients if they request customer data from competitors to compete for new customers, or to win back customers that they have previously lost.
184. It is possible that the ecosystem could develop around trusted data platforms, which connect customers, data holders and users with multiple types of data and assist multiple different data uses.

perspective. These concerns are already managed in other important sectors of our economy and these risks are articulated clearly and managed carefully in our payment systems, clearing systems and financial markets through standards such as the Principles of Financial Market Infrastructure.[185] It will be a new, and necessary, challenge of the future to apply those frameworks to data.

Greater transparency in the value of data

The PC Data Report noted that there were two obvious conclusions in relation to the value of data:

> *First, the potential value of data, by some estimates is immense; second it is impossible to be definitive about this value, particularly when it requires speculation about possible current and future uses.*[186]

The substantial value of data was also a point made in many submissions, as was the potential lack of understanding of that value by consumers. This disparity between recognition of value, and difficulty in determining it, arises because when considered as an asset, data has particular characteristics:

- its value will differ between users, based on their use of it
- it is not depleted by being shared with someone else
- it can be refined and improved from its raw form
- there is no transparent marketplace for data, and
- it is an illiquid asset, and data transactions are complex and time consuming.[187]

This difficulty in valuation can be considered an impediment to appropriate dealing with data, from both a customer and a business perspective. The inability for a customer to determine a value for their data means that decisions about sharing it with others cannot be made on a truly informed basis, as the consumer cannot be sure that it is receiving suitable value in exchange for what they are providing. This is made more challenging where anything exchanged for data is itself not easily valued, so that there is no basis to value either side of the transaction. As a result of this, a customer's data could be perceived as having no real value, or worth. Further, this perception of no value can result in customers perceiving that there is less need for responsibility in making choices in relation to their data. The inability to properly value data impedes efficiency in its sharing.

Establishing a means of transparently valuing data would be beneficial.[188] There are many methods which can be taken to value assets, including ones for assets which do not have a liquid market. The Review considers that improving the transparency in the value of data would assist the effectiveness of Open Banking. To the extent that Open Banking leads to the safe and efficient

185. The Principles of Financial Market Infrastructure are produced by Bank for International Settlements (BIS) and International Organization of Securities Commissions (IOSCO). They are international standards used for important multilateral systems and are adopted in Australia's most important financial systems. They are comprised of a number of principles, including the need for a sound risk-management framework for comprehensively managing legal, credit, liquidity, operational and other risks.
186. PC Data Report, page 117.
187. These points are taken from the White Paper published by Data Republic: 'How much is your company's data really worth? Data pricing and valuation in the age of the data economy' September 2017, Available at: https://www.datarepublic.com/assets/data-republic-company-data-worth.pdf
188. Comments on connection between the generation awareness around the value of data and positive consumer outcomes were made in the submission of the Australian Payments Council, page 6.

transfer of data, it could assist in working towards the goal of providing customers with visibility of the value of their data.[189] Further, the creation of a new data ecosystem could also lead to the development of more liquidity and transparency in the exchange of data, which should assist value discovery.

Interoperability with other jurisdictions

Where regulatory requirements are similar across jurisdictions it makes it easier and quicker for jurisdictions to establish their regimes. It also enables businesses that want to operate in more than one jurisdiction to only have to create one set of procedures that comply with each jurisdiction's requirements. However it does not enable that jurisdiction to incorporate features that reflect the national character or take into account existing regulatory and other structures.

Bespoke frameworks can make it difficult for businesses to operate across jurisdictions due to the need to put in place extra arrangements that comply with other jurisdictional requirements. Bespoke frameworks also limit competition from businesses outside of the jurisdiction.

As discussed earlier in this Report, jurisdictions have taken different approaches in their implementation including, the scope of application, the stringency and degree of prescription of standards and the degree of compulsion of implementing that suit their region's circumstances.

Some submissions have advocated that Australia use already tested standards to enable a faster approach to implementation.[190] Others prefer that Australia take a more selective approach that gives primacy to ensuring the security of customer data.[191]

Australia's approach to Open Banking, as set out in this Review, reflects a blend of international interoperability and Australia's unique circumstances. The Review has endorsed pursuing interoperability with other countries, but only to the extent that interoperability aligns with Australia's interests or would have customer support. Regulatory authorities and policy makers should be alert to regulatory frameworks and models for best practice internationally that may be applicable in Australia but also seek to achieve better outcomes wherever possible.

189. This connection between strong and transparent governance and customers' recognition of value of data was made in the Westpac submission, page 14.
190. FinTech Australia submission, page 22.
191. ABA submission, page 3.

Glossary

Accredited party:	A party who has satisfied the accreditation criteria set by the ACCC and can, as a result, enter into data sharing arrangements under Open Banking.
Address book:	The list of Open Banking accredited parties maintained by the ACCC, specifying their level of accreditation.
Aggregated data set:	Data sets that use multiple customers' data to produce de-identified, collective or averaged data across customer groups or subsets.
Application programming interface (API):	Software designed to help other software interact with an underlying system.
Australian Financial Complaints Authority (AFCA):	A new external dispute resolution scheme to resolve disputes about products and services provided by financial firms.
Australian Privacy Principle (APP):	Outline how most Australian and Norfolk Island Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses must handle, use and manage personal information.
Credit and Investments Ombudsman:	An independent industry ombudsman dispute resolution scheme for consumers who are unable to resolve complaints with member financial service providers.
Commencement Date:	The first day of operation of Open Banking in Australia.
Consumer Data Contact Point:	A virtual point of contact, such as a single telephone number and webpage, which connects complainants to complaint handlers.
Consumer Data Right:	The right of Australian consumers to have open access to their data. The Consumer Data Right was a recommendation of the PC Data Report and the Government has announced it will legislate for this right and implement it sector-by-sector, beginning in the banking, energy and telecommunications sectors.
Customer-provided data:	Information provided by customers to their bank.
Data holder:	A party that holds data to which the Consumer Data Right will apply.
Data recipient:	A party that is accredited to receive data under the Consumer Data Right.

Data Standards Body:	A body to be established to set Standards for the Consumer Data Right and Open Banking.
Extensibility:	The capacity of a system to be adapted for different purposes.
Financial Ombudsman Service:	An independent industry ombudsman dispute resolution scheme for consumers who are unable to resolve complaints with member financial service providers.
Fingleton Report:	*Data Sharing and Open Data for Banks* report published by the Open Data Institute and Fingleton Associates in 2014 (UK).
Interoperability:	The ability of software systems to exchange information efficiently.
Middleware:	Software that acts as an intermediary between other systems.
OAuth 2.0:	A widely adopted framework for providing delegated authorisation.
Open Banking:	A system to give customers access to and control over their banking data and data on banks' products and services.
Participants:	All persons and entities (including customers) involved in Open Banking.
Passporting:	Mutual recognition of accredited parties by different systems.
PC Data Report:	*Data Availability and Use*, Productivity Commission Inquiry Report No. 82, 31 March 2017
Phishing:	The attempt by a bad actor to gain a user's credentials by posing as a trusted party.
Product data:	Information about banking products that banks and other financial service providers are bound by legislation to disclose about those products, such as details on their price, fees and charges.
Read access:	Access to view data, but not to initiate payments.
Reference data:	Includes information on branch and ATM location and certain product information
RESTful APIs:	Stands for REpresentational State Transfer APIs, which follow the design principles that underpin the World Wide Web.
Rules:	Rules for Open Banking, addressing customer rights, competition and confidentiality. The Rules are to be written by the ACCC, in consultation with the OAIC and other relevant regulators.

Sandbox:	A version of a system created to allow new software to be tested without affecting the system that is being used to provide services to customers.
Screenscraping:	The practice of third parties using a customers' login credentials provided by customers to extract banking data (such as account balance and transactions) from the information that the customer may see on their internet banking screen.
Standards:	Specific direction for participants on how to connect, transfer and satisfy the Rules written by the Data Standards Body. The Standards should include detailed information on engineering, technology, data and security.
Transaction data:	Data that is generated as a result of transactions made on a customer's account or service.
Use case:	Where a particular data set has a current and demonstrable application to the provision of a financial product or service.
Value-added customer data:	Data that has been enhanced by a data holder to gain insights about a customer.
Write access:	Access to initiate payments from a customer's account.

Key Acronyms

ACCC	Australian Competition and Consumer Commission
ADI	Authorised Deposit-taking Institution
AML/CTF	Anti-Money Laundering and Counter-Terrorism Financing Act 2006
API	Application programming interface
APP	Australian Privacy Principle
APRA	Australian Prudential Regulation Authority
ASIC	Australian Securities and Investments Commission
ATM	Automated teller machine
CCA	*Competition and Consumer Act 2010*
CDR	Consumer Data Right
CIO	Credit and Investments Ombudsman
EBA	European Banking Authority
EDR	External Dispute Resolution
EU	European Union
FCA	Financial Conduct Authority (UK)
FOS	Financial Ombudsman Service
FSI	Financial System Inquiry
GDPR	General Data Protection Regulation (EU)
IDR	Internal Dispute Resolution
KYC	Know Your Customer
OAIC	Office of the Australian Information Commissioner
OBIE	Open Banking Implementation Entity (UK)
OBWG	Open Banking Working Group (UK)
ODI	Open Data Institute
OFX	Open Financial Exchange
PC	Productivity Commission
PSD2	Payment Services Directive 2 (EU)
RBA	Reserve Bank of Australia
SME	Small-to-medium enterprises

Appendix A: Terms of Reference

Purpose of the Review

The Government will introduce an open banking regime in Australia under which customers will have greater access to and control over their banking data. Open banking will require banks to share product and customer data with customers and third parties with the consent of the customer.

Data sharing will increase price transparency and enable comparison services to accurately assess how much a product would cost a consumer based on their behaviour and recommend the most appropriate products for them.

Open banking will drive competition in financial services by changing the way Australians use, and benefit from, their data. This will deliver increased consumer choice and empower bank customers to seek out banking products that better suit their circumstances.

Terms of Reference

1. The review will make recommendations to the Treasurer on:

    1.1 The most appropriate model for the operation of open banking in the Australian context clearly setting out the advantages and disadvantages of different data-sharing models.

    1.2 A regulatory framework under which an open banking regime would operate and the necessary instruments (such as legislation) required to support and enforce a regime.

    1.3 An implementation framework (including roadmap and timeframe) and the ongoing role for the Government in implementing an open banking regime.

2. The recommendations will include examination of:

    2.1 The scope of the banking data sets to be shared (and any existing or potential sector standards), the parties which will be required to share the data sets, and the parties to whom the data sets will be provided.

    2.2 Existing and potential technical data transfer mechanisms for sharing relevant data (and existing or potential sector standards) including customer consent mechanisms.

    2.3 The key issues and risks such as customer usability and trust, security of data, liability, privacy safeguard requirements arising from the adoption of potential data transfer mechanisms and the enforcement of customer rights in relation to data sharing.

    2.4 The costs of implementation of an open banking regime and the means by which costs may be imposed on industry including consideration of industry-funded models.

3. The review will have regard to:

    3.1 The Productivity Commission's final report on Data Availability and Use and any government response to that report.

    3.2 Best practice developments internationally and in other industry sectors.

    3.3 Competition, fairness, innovation, efficiency, regulatory compliance costs and consumer protection in the financial system.

Process

The review will consult broadly with representatives from the banking, consumer advocacy and financial technology (FinTech) sectors and other interested parties in developing the report and recommendations.

The review will report to the Treasurer by the end of 2017.

Appendix B: Consultation

On 20 July 2017, the Treasurer, the Hon Scott Morrison MP, announced the Terms of Reference for the Review and the appointment of Mr Scott Farrell as the independent expert to lead the Review.

The Review published an Issues Paper with public comment invited from 9 August 2017 to 22 September 2017.

The Review received 40 public submissions (including one anonymous submission) and one confidential submission in response to the Issues Paper. Two entities provided supplementary submissions to their original submission. Submissions ranged from interested individuals, online service providers, stakeholder groups, government agencies and banks. All public submissions have been placed on the Review website.[192]

The Review also conducted more than 100 meetings during the five months since the Review was commissioned. The Review held one-on-one meetings with interested parties in Melbourne, Sydney, Canberra and London. Roundtables meetings were also held in Melbourne, Sydney and Canberra.

Table B.1: Organisations and individuals who provided submissions

Organisations and individuals
Acorns Grow Australia
American Express Australia
Australia and New Zealand Banking Group
Australian Bankers' Association
Australian Finance Industry Association
Australian Payments Council
Australian Payments Network
Australian Privacy Foundation
Australian Securities and Investments Commission
Australian Small Business and Family Enterprise Ombudsman
Business Council of Australia
Business Council of Co-operatives and Mutuals
Commonwealth Bank of Australia
Consumer Action Law Centre, Financial Rights Legal Centre and Financial Counselling Australia
Cuscal

192. Available at: https://treasury.gov.au/review/review-into-open-banking-in-australia/

Organisations and individuals
Customer Owned Banking Association
Elliston, Ben
Envestnet Yodlee
Experian Australia
FinTech Australia
Fitzgerald, Mark
ID Exchange
King & Wood Mallesons
Lawsoft
Metcalf, Belinda
Moneytree Financial Technology
National Australia Bank
Office of the Australian Information Commissioner
PayPal Australia
Raidiam
Regional Australia Bank
Reserve Bank of Australia
SMSF Association
TransferWise
Verifier
Westpac Group
Xero Australia

Appendix C: Open Banking in other jurisdictions

Globally, Open Banking initiatives are most advanced in the European Union (EU), the United Kingdom (UK) and the United States (US), but are also emerging in many other jurisdictions.

The UK is unique in having the only Government-mandated Open Banking system. In the EU, the Payment Services Directive 2 (PSD2) and General Data Protection Regulation (GDPR) are set to open up the banking market while strengthening consumer protections when they both come into effect in 2018. Open Banking in the US has been driven by the emergence of FinTechs who have accessed consumer data by screenscraping, a practice which is now changing as bilateral agreements between banks and FinTechs become increasingly popular. Following, in part, the effect of PSD2 and GDPR, governments in Hong Kong, India, Japan, New Zealand and Singapore have also put in place frameworks which will support Open Banking.

Although there are some commonality between the Open Banking frameworks developing in other countries (such as customer choice), there is no single model which is being consistently adopted. The approach taken in each jurisdiction reflects important features of the jurisdiction, including the structure of the jurisdiction's data, privacy, competition and banking laws, the development of the FinTech industry and the structure of the local banking industry.

Europe under Payment Services Directive 2 and General Data Protection Regulation

The EU's banking framework is set to fundamentally change in 2018, with the PSD2 and the GDPR both coming into force. PSD2 aims to open up the European banking landscape by increasing efficiency, competition and security for payments and GDPR will enforce stronger data security and privacy protections for personal data.

EU member states must implement GDPR via their own national law by 25 May 2018. GDPR is a single set of rules, applicable to all EU member states, regulating data protection for all individuals in the EU. It broadens the scope of existing EU law by introducing new consumer data rights, including the right to deletion, the right to direct their data be shared and the right to object to profiling.[193] It will also govern consent, privacy and liability.

PSD2 will apply to all EU member states, incorporated in their own national laws, from 13 January 2018. It gives customers the ability to grant third parties read and write access to their banking data via open APIs. This means third parties can see and use customer banking data and also make payments on behalf of the customer. Initially, PSD2 will not prohibit screenscraping. However, this

193. Data processing may be characterised as profiling when it involves automated processing of personal data and using that personal data to evaluate certain personal aspects relating to a natural person.

practice will become less accessible when the regulatory technical standards take effect in mid-2019. In the longer term, as open APIs become established, PSD2 aims to make screenscraping redundant. PSD2 requires Strong Customer Authentication (SCA). This means the customer's identity must be verified through two or more authentication tools each time they request access. It also requires the provision of internal dispute resolution.

United Kingdom

The UK has been an early implementer of mandated Open Banking. Under the UK's Open Banking system, the nine largest UK banks[194] are required to share data with authorised third parties using secure open APIs at the customer's direction. Legislation governing Open Banking in the UK is effectively an amalgam of UK-specific laws and the EU's PSD2 and GDPR legislative framework described above.

Open Banking in the UK began with the release of the Fingleton Report in 2014.[195] This report considered the competitive and consumer outcomes of banks sharing transaction data with third parties using APIs. Its recommendations — including an industry-led agreement on an open API standard to facilitate data access for third parties and an industry-wide approach for authorising third parties — laid the foundations for Open Banking in the UK. Following these recommendations, the UK Treasury established the Open Banking Working Group (OBWG) to define Open Banking policy, standards and frameworks. The OBWG's recommendations were adopted and legislated by the Competition and Markets Authority (CMA) in 2016.

As the first phase of implementation, in March 2017 nine banks were required to make access available to non-sensitive data — branch and ATM locations as well as product and fee information for specific accounts[196] — via open APIs. In January 2018, the data scope will broaden, with customer and transaction data[197] to become available, but only for personal and SME current accounts (that is, transaction accounts). This second phase of UK Open Banking will also allow write access for authorised participants through secure open APIs, allowing them the ability to initiate payments from customer accounts.

The UK has established the Open Banking Implementation Entity (OBIE) as the delivery entity for UK Open Banking. It was required by the CMA, is led by an independent trustee and funded by the nine largest banks. The decisions of the OBIE are made by the Implementation Entity Steering Group (IESG), whose members are the nine largest banks, five advisory groups, two consumer representatives and an observer from each of HM Treasury, the Payment Systems Regulator, the Financial Conduct Authority and the Information Commissioner's Office.[198]

Third parties that use published APIs to access customer data will be authorised and regulated by the Financial Conduct Authority (FCA) and enrolled on the Open Banking Directory. This directory provides the identity records and digital security certificates required to operate in the Open Banking

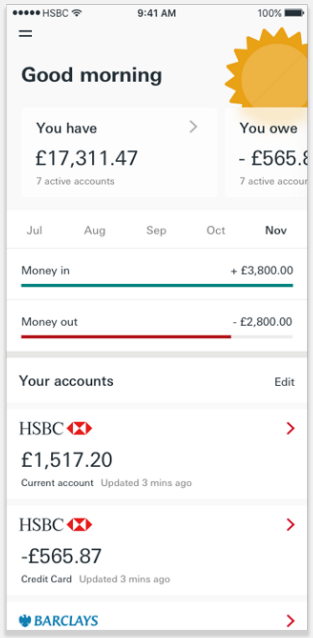
194. HSBC, Barclays, Lloyds Bank, RBS, AIB, Nationwide, Santander, Bank of Ireland and Danske Bank.
195. Commissioned by HM Treasury.
196. Personal Current Accounts, Business Current Accounts (SME's), Unsecured lending (SMEs).
197. For personal and business current accounts.
198. Available at: https://www.paymentsuk.org.uk/sites/default/files/Implementation%20Entity%20Steering%20Group%20-%20Oct%202016%20Update%20to%20CMA.pdf

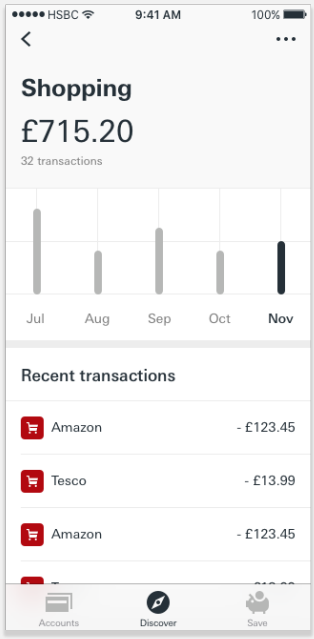
system. Third parties can be an account information service provider (AISP) or a payment initiation service provider (PISP) or both. AISPs have account read access and PISPs have account write access.

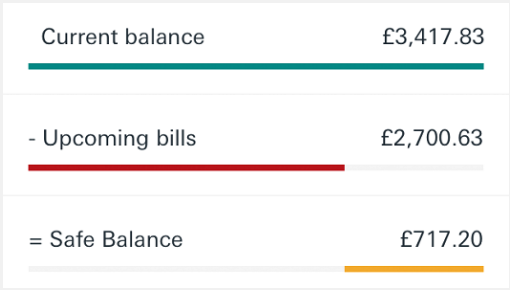
Box C.1: HSBC Beta app

An early insight into what may lay ahead for consumers under Open Banking in the UK is the Beta app, launched by HSBC in September 2017 and currently being trialled by 10,000 of its customers. Beta provides HSBC customers a consolidated view of their bank accounts held with up to 21 different banks. The account categories covered by this app are wider than those mandated by the CMA for inclusion in the UK's Open Banking reform.

Beta provides some value-adding services, such as 'safe balance', which shows how much cash the user has left until payday, and a nudge feature, which will let the user know if they exceed their spending limits.







United States

Open Banking in the US is emerging organically, mostly via bilateral data sharing agreements, driven by innovative FinTechs and commercial incentives of incumbent banks to seek new competitive advantages. While there has been no specific regulatory or legislative framework implemented to support Open Banking, the Consumer Financial Protection Bureau (CFPB) has published non-binding principles aimed at the 'consumer-authorised data-sharing market'. These principles advocate giving consumers access to their own data in a useable format and allowing consumers to authorise (and revoke) read-only third party access. They also promote informed consumer consent, data security, and dispute resolution and suggest protocols on data use and retention as well as liability.

FinTechs in the US have historically accessed consumer data by screenscraping. Limitations in this practice have emerged for both banks and FinTechs. In 2015, several of the big banks (Wells Fargo, JP Morgan Chase and Bank of America) temporarily blocked data access to screenscrapers citing security and bandwidth concerns. Whilst access was soon restored, FinTechs are increasingly struggling to meet their customers' demand for access to secure real-time data using screenscraping.

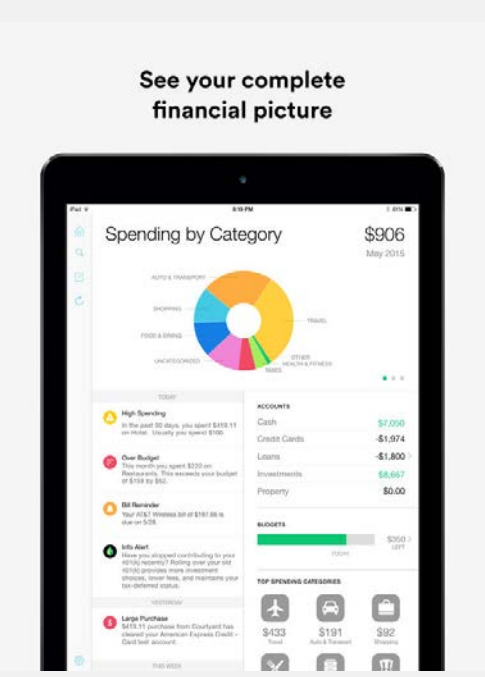
The banks are now moving the market away from screenscraping by negotiating bilateral agreements with FinTechs, thereby allowing data sharing using APIs. JP Morgan Chase has been particularly active in working with third parties to move away from data sharing via screenscraping in favour of secure APIs. In a 2015 letter to shareholders, JP Morgan Chase CEO Jamie Dimon made specific note of the company's desire to move towards systems that "allow us to 'push' information – and only that information agreed to by the customer – to that third party". [199] At the beginning of 2017 JP Morgan Chase signed a data sharing agreement with US business and financial software company Intuit. In July 2017 they signed another, similar, agreement with Finicity.

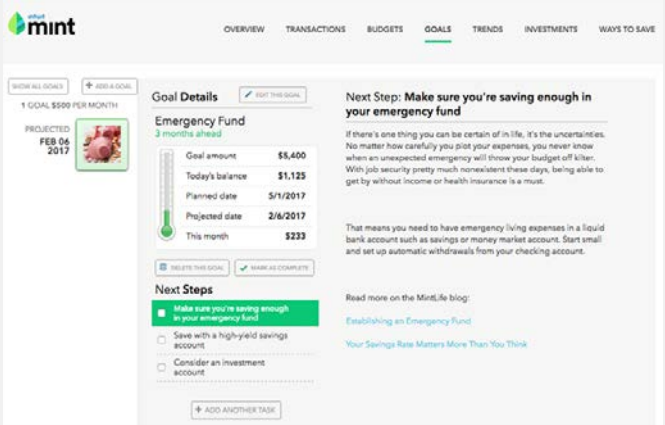
Other US banks that have been actively pursuing bilateral data sharing arrangements with FinTechs include Citigroup, Wells Fargo and Bank of America.

Box C.2: Mint

Mint has been a pioneer in customer data sharing in the US. It was created in 2006 as an account aggregator service (website and app). Mint's subscribers were able to see all their accounts through a single user interface. Its subscriber numbers grew quickly and, in 2009, Mint was acquired by Intuit. In 2016, Mint reported more than 20 million users across North America.

Early 2017, Intuit announced bilateral agreements with both Wells Fargo and JP Morgan Chase. This means bank customers can authorise the bank to share their data with any or all of Intuit's apps (Mint, TurboTax and Quick Books) using the banks' APIs.





199. Available at: https://www.jpmorganchase.com/corporate/investor-relations/document/2015-annualreport.pdf

Hong Kong

Hong Kong is moving closer to Open Banking. In September 2017, the Hong Kong Monetary Authority (HKMA) announced it was developing a policy framework aimed at the development and use of API's in the banking sector. The HKMA is currently consulting with banks and the details of this framework are expected to be announced by the end of 2017. The HKMA has also announced other initiatives that will support Open Banking, including payment reforms and incentives for FinTech firms to set-up and operate in Hong Kong.[200]

Japan

Open Banking in Japan is in its early stages. The Japanese Prime Minister, Shinzo Abe, made specific references to Open Banking initiatives in his 2017 Growth Strategy, setting a target of open API systems in more than 80 banks by 2020.

Consistent with this aspiration, several key amendments to the Banking Act were recently passed that support the development of Open Banking. In 2016, an amendment was passed that makes it easier for banks to invest in FinTech firms by freeing up shareholding restrictions. In May 2017, another amendment was passed aimed at promoting affiliation and co-operation between banks and FinTech firms. This amendment requires financial institutions that intend to execute contracts with payment providers to make efforts to develop a system that enables open APIs within a two year timeframe.

In June 2017, IBM Japan announced the launch of API banking for Mizuho Bank.

New Zealand

New Zealand is exploring the idea of Open Banking. Payments NZ[201] is currently investigating making payments through a shared API framework as part of wider payments reforms.[202]

FinTech firms are also becoming active in Open Banking. Revolut will make their payments platform available in New Zealand in 2018. Smartpay has recently launched digital payment software that works like an open API. Start-up FinTech, Jude, has announced plans to launch an aggregator service in early 2018, using screenscraping to access customer banking data.

The New Zealand Government has not made any formal announcements on Open Banking to date.

Singapore

There is no government-mandated Open Banking in Singapore. However, the Singapore Government has demonstrated strong support for development of the FinTech industry and this support includes some Open Banking type initiatives.

200. Available at: http://www.hkma.gov.hk/eng/key-information/press-releases/2017/20170929-3.shtml
201. Payments NZ is the organisation that governs the New Zealand payments system. Its shareholders are ANZ, ASB, BNZ, Citibank, HSBC, Kiwibank, TSB Bank and Westpac.
202. Available at: https://www.paymentsnz.co.nz/about-us/payments-direction/

The Monetary Authority of Singapore (MAS) and the Association of Banks in Singapore jointly developed and published non-binding API guidelines in 2016. [203] These guidelines offer comprehensive advice on API development and implementation as well as information on security standards and governance models. Citibank, OCBC, Standard Chartered and the MAS have published open APIs, as recorded on the MAS Financial Industry API Register.

Other initiatives that may encourage the development of Open Banking include the 2016 launch of a regulatory sandbox for developers, the establishment of a 'one-stop-shop' for FinTechs in Singapore (including seed capital), cloud computing guidelines, the development of a Strategic Electronic Payments system and plans for the creation of a national Know-Your-Customer utility.

India

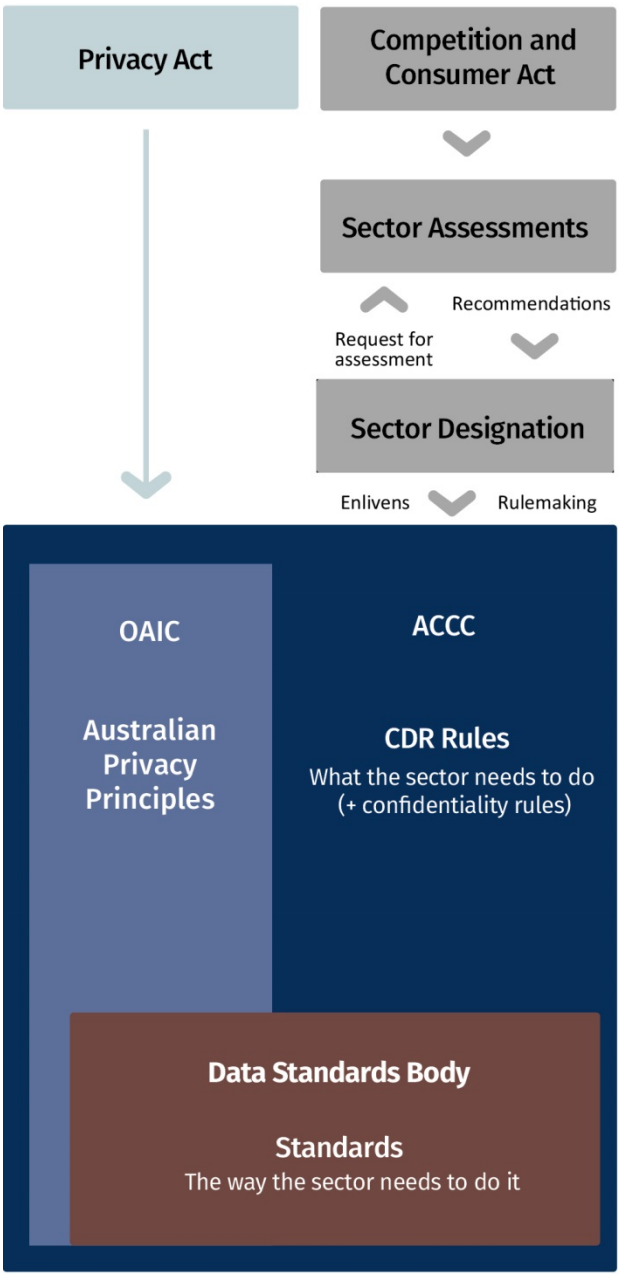
The possibility of Open Banking in India is being paved by the Unified Payments Interface (UPI), a system that has the potential to transform India's payments system. India is seeking to move away from a cash-based economy to an instant, real-time payment system where funds are transferred between two bank accounts using a mobile phone app.

The UPI is underpinned by the ongoing roll out of a 12-digit unique identifier (UID or "Aadhaar") to all Indian residents. The UID is an identifier based on fingerprint, iris and facial features and is used to authenticate the user. Once this biometric authentication has taken place, any Indian resident with a smart device and an internet connection can (in theory, at least) make UPI payments.

There is evidence that Indian banks are investigating Open Banking. India's largest bank, the government-owned State Bank of India, opened its APIs for a hackathon in 2017 and has stated its intention to hold hackathons quarterly in a bid to collaborate with developers and FinTechs. Other government owned banks — RBL and Axis Bank — have also opened their APIs for hackathons.

203. Available at: https://abs.org.sg/docs/library/abs-api-playbook.pdf

Appendix D: Recommended regulatory framework for Open Banking



- Outlines Principles and regulatory framework
- Creates statutory right and power for Minister responsible for competition to designate sectors or data sets
- Banking is pre-designated in regulation accompanying amendments to the CCA

- Banking does not require a sector assessment
- For other sectors, assessments undertaken by ACCC in consultation with OAIC and relevant regulators, either at Minister for competition's request, ACCC's initiative, or at sector's request

- Minister has power to designate sectors
- Designation turns on rule-making for specified classes of entity and data e.g. banks and data as scoped
- Minister for competition may make regulations to restrict rule making powers

- ACCC makes Rules, in consultation with public, OAIC and relevant regulators.
- Rules set out:
  - who is bound by the CDR system, and the specific data sets that are covered
  - the outcomes that must be met by the transfer mechanism in order to support competition and promote good customer outcomes
  - accreditation criteria
  - rules governing infrastructure (including when it is needed)
- Ministerial consent is required for Rules.
  - Rules submitted for consent must be accompanied by regulatory impact assessments and OAIC privacy impact assessment
- The ACCC is responsible for ensuring, but not necessarily providing, accreditation and maintenance of the address book, including decisions to add or remove parties from the address book.

- Data Standards Body is to co-ordinate transfer, data, security and like standards, and developer resources including ensuring that technology sandboxes are provided.
- The Data Standards Body has an independent chair, appointed by Government
- Binding once:
  - OAIC assessment of compliance with privacy law
  - ACCC assessment of compliance with Rules

Complaints and Enforcement

Consumer Data Contact Point

- A single point of access for consumer complaints
- OAIC handles customer complaints under CDR
- Customers have standing to seek remedy
- OAIC reports all complaints to the ACCC to monitor systemic and competition issues

External Dispute Resolution

- Provides individual remedies
- Existing EDR used where appropriate. FOS and CIO (soon to be AFCA) currently approved EDR providers under Privacy Act
- EDR would extend to SMEs for confidentiality issues
- Accredited parties agree to undertake EDR to resolve disputes between themselves

Enforcement

- Ensures CDR system as a whole works
- ACCC enforces the Rules
- ACCC enforces specific requirements regarding the 'infrastructure' supporting the market
- ACCC enforces existing competition laws and systemic CDR issues
- OAIC enforces Privacy Law, responsible for systemic enforcement of privacy and confidentiality

Appendix E: Example Rules and topics

Part 1: Example Rules for the Consumer Data Right — direction to transfer

Part 1 presents example Rules for the Consumer Data Right on the direction to transfer to illustrate the level of detail the Review recommends be reflected in the Rules.

Direction to Transfer

Nature of direction

A. Express (not implied) direction from the customer must be obtained by the data holder to transfer data to an accredited recipient.

B. Direction must be informed, unambiguous and specific.[204]

   i. The customer must be presented with such information as approved by the ACCC in the manner approved by the ACCC.

   ii. The ACCC may specify that the customer must acknowledge having received or being aware of relevant information in order for direction to be validly given.

C. Directions to transfer must not be bundled either with other directions, permissions, or other agreements.

D. For joint accounts, the person or persons with the authority to direct actions on the account has the authority to direct the transfer of data.

   i. Where any account holder may direct actions on the account, any account holder may direct the transfer of data.

   ii. Where more than one account holder must consent to direct actions on the account, that number of account holders must direct the transfer of data.

E. The consent of the counterparty to a transaction with the customer is not required for the transfer of data in relation to that transaction.

F. A customer's direction to transfer must expire at least before the maximum of a period of time as determined by the ACCC.

   i. This does not affect the liability of the customer to any other entity under any agreement or obligation to provide access for any longer period.

204. Note: These terms would be further defined by regulator guidance.

G. Those holding authority to act on behalf of a person, for example Powers of Attorney, and those acting as agents within their authority are able to give direction on behalf of the customer.

Process for obtaining direction to transfer

H. Customers must be able to provide their direction to the data holder in a way that is timely; efficient; and convenient.[205]

I. Directions to transfer must be able to be provided in a manner that is no more onerous than the customer's usual method of authorising actions on their account.

J. If the data holder already provides online mechanisms for the customer to perform actions on the account, the data holder must allow the customer to direct transfer to a data recipient through this online mechanism.

K. At the time of direction, the data holder must present the customer with the ability to nominate which data sets they wish to share and the duration of access they are granting.

L. A customer's direction to a data holder to share their data must be able to be provided in a way that does not unduly disrupt the client experience with the data recipient. In particular:

    i. The direction process must not involve any more than is necessary or required by the rules to obtain direction.

    ii. The direction must be able to be provided in a way that does not unduly interpose the data holder into the customer's client experience with the data recipient.

    iii. Information provided to the customer by the data holder as part of the process of obtaining direction must not be misleading.

M. A customer's direction must be able to be provided in a way that does not require the data holder to be informed, or approve, of the purpose of the data transfer.

N. Joint account holders must be notified by the data holder upon direction being given, amended or cancelled and be able to amend or cancel data sharing arrangements initiated by other joint account holders who have the authority to direct the transfer of data.

O. Provided it is consistent with the customer's direction, the direction to transfer must be able to effect subsequent data transfers without requiring re-authentication and re-authorisation from the customer.

P. A customer must be able to withdraw their direction easily and with near immediate effect.

    i. Withdrawal of direction must be able to be effected through the data holder or through the data recipient.

205. The Standards specify the method by which accredited parties demonstrate compliance with this and other rules.

ii. This rule does not affect the liability of the customer to any other entity under any agreement or obligation to provide access for any longer period.

Authentication when directing transfer

Q. The direction to transfer must incorporate a timely; efficient; convenient; safe and reliable method for authenticating the identity of the customer with a level of assurance that is commensurate with the risks associated with the proposed data transfer.

R. Nothing in these rules precludes the direction to transfer from permitting or compelling reliance on identity service providers other than the data holder for authentication.

Record Keeping

S. Accredited parties must record, and make available in an accessible form to customers, all directions sought, given, refused, modified or revoked.

T. Accredited parties must retain for a period of time as defined by the ACCC and make available to the ACCC on request, the terms (but not content) of all data requests and responses sought, given or refused.

Part 2: Topics of the Rules

Part 2 lists the topics that the Review has recommended should be included within the Rules. These are not worded as the Rules would be expected to be worded, but are based on the recommendations in the Review. The Review has provided this list as a starting point for the ACCC's consultation and to provide further guidance to interested parties. This list is not exhaustive and additional issues are expected to be added through the consultation process.

Objectives of the system

The rules would include objectives to help guide the interpretation of other rules. It is likely that this would include similar objectives to those of the UK system, including concepts of openness; usability; interoperability; reuse; independence; extensibility; stability; and transparency.

Scope of the right

The rules would outline that customers have the right to access and direct the transfer of designated data sets about them to accredited parties in a form that facilitates their transfer and use. It would also define:

- the limits of the Consumer Data Right
- who the Rules apply to
- the hierarchy of general Consumer Data Right Rules, sectoral Rules, and other relevant law including the *Privacy Act 1988*, and
- sector specific detail of data and entities covered.

Direction to Transfer

- See Part 1 for example rules regarding direction to transfer.

Authentication

- See Part 1 for example rules regarding authentication.

Permission to Use

The rules would outline that though the data recipient does not need to inform the data holder of all intended uses, there are prescribed uses that should be presented to the customer for permission (consent) to be considered informed. These uses would be expected to include:

- the primary purpose for which the data is being transferred
- on-selling of data
- direct marketing
- transfer of data outside of the Consumer Data Right system, and
- transfer of data overseas.

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

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

Transfer

The rules would stipulate that transfer pursuant with the Consumer Data Right, including responses to transfer requests, must occur in accordance with the relevant sectoral Standards, as defined by the Data Standards Body. This would include rules regarding: what can be transferred based on the data recipients level of accreditation; security requirements for data in transit; that in instances of transfer between sectors, the relevant Rules and Standards are the sectoral Rules and Standards of the data holder's sector; and dealing with unsolicited information.

Security

The rules would outline requirements for dealing with information received under the Consumer Data Right, including: treatment of potentially sensitive, harmful, or commercially damaging information. It would also outline that data received under the Consumer Data Right must only be kept for as long as is necessary to meet the purpose(s) that the data was transferred; and that information transferred under the Consumer Data Right must be protected from interference, misuse and loss, unauthorised access, unauthorised modification and disclosure.

Risk management

The rules would require accredited parties to have sufficient systems and resources in place to comply with the *Privacy Act 1988* and the Consumer Data Right rules. This may include rules about the use of outsourcing arrangements where the outsourcing provider holds data on behalf of the accredited party, but is not itself accredited.

Breach reporting

The rules would outline circumstances in which accredited parties must report breaches of the Consumer Data Right. This may include expanding upon the *Privacy Amendment (Notifiable Data Breaches) Act 2017*.

Fraud and misconduct

The rules would outline circumstances that may amount to a contravention of a civil penalty provision, or an offence. This may include: purporting to be accredited when not accredited; interference with the address book; release or publication (otherwise than in accordance with law) of information received under the Consumer Data Right; interception or interference with data transferred under the Consumer Data Right; and refusal to transfer to an accredited party (otherwise than in accordance with law).

The rule would also outline remedies available under the civil penalty provisions.

Record keeping

The rules would outline record keeping requirements, what records need to be made available to customers and regulators, and for how long. For example, records of consents given.

Accreditation criteria

The rules would outline that the ACCC has the power to determine the risk level of a data set and impose a tiered system of accreditation reflecting these risks.

The rules would require that all parties be accredited to be able to receive data under the Consumer Data Right and the criteria to be accredited to different tiers, based on the assessed risk level of that data.

Accreditation governance

The rules would outline accreditation governance requirements including who can make accreditation decisions and processes to appoint competent authorities to make accreditation decisions, time periods for decisions, the publication of accreditation guidelines, and that accreditation decisions are reviewable by the Administrative Appeals Tribunal.

Address Book

The rules would outline what must be reflected on the address book (register of accredited participants), who has power to alter the address book, the process for being appointed to alter the address book, the legal effect of relying upon the address book, and that the address book must be publicly available, and up to date.

Data Standards Body

The rules would outline the role and functions of the Data Standards Body, including the objectives that the Data Standards Body should promote in setting the Standards and its powers to set and publish Standards related to data security, transmission of data, and data formats. The rules would also outline the legal effect of the Standards.

Data Standards Body governance and standard-setting processes

The rules would outline the minimum governance arrangements of the Data Standards Body, and obligations of the Data Standards Body, including in relation to consultation, reporting, publication and timelines.

Dispute Resolution

The rules would outline requirements for data providers and accredited parties to provide (and publish processes for) Internal Dispute Resolution and External Dispute Resolution.

Mutual recognition of foreign regulatory regimes

The rules would outline when the ACCC may recognise foreign regulatory regimes for data sharing and 'passport' the accreditation of foreign parties.