ASIC

Australian Securities & Investments Commission

# Review into Open Banking in Australia

# Submission by the Australian Securities and Investments Commission

September 2017

# Contents

# Executive summary

1 ASIC supports the Government's Review into Open Banking in Australia (Review) and welcomes the opportunity to contribute to its examination of the most appropriate model and implementation approach for Australia.

2 Open Banking has the potential to help empower consumers in their decision making, stimulate competition and innovation within the financial services sector, and support better decision making and risk management by financial institutions.

3 Open Banking is an emerging and evolving concept. Different jurisdictions are currently at varying stages in introducing Open Banking, with diverse approaches to design and implementation. ASIC understands that these different approaches have affected the scope of each regime and the potential benefits and risks for consumers.

4 Depending on how an Open Banking regime in Australia is designed and regulated, the regime could give consumers (and third parties they nominate) access to their financial services data in a secure environment.

5 Access to this information would potentially allow consumers to:

(a) make more informed financial decisions; and

(b) access a wider range of products and services that are tailored to their needs and/or that deliver better value for money.

6 In Section A of this submission, we examine:

(a) some suggested objectives that an Open Banking regime in Australia could seek to achieve;

(b) the potential benefits of an Open Banking regime, depending on those objectives; and

(c) other design considerations we consider to be important, including consumer behavioural factors, the development of common technical standards for technology, data and security, and how the regime could be implemented.

7 In Sections B and C of this submission, we look at:

(a) the need for a cohesive framework for regulation and oversight to ensure consumers can have trust and confidence in the regime; and

(b) the potential scope and coverage of the regime, including types of financial institutions, types of data sets and third party providers.

8 Table 1 summarises ASIC's views on these key issues and factors.

**Table 1: Summary of key issues and factors for an Open Banking regime in Australia**

| Issue | Key factors |
|---|---|
| **Design of an Open Banking regime in Australia** (see Section A) | An important starting point in developing an Open Banking regime in Australia is to set a clear list of objectives as the regulatory model chosen for Open Banking will ultimately depend on what the regime is intended to achieve and its design.<br>There is potential for Open Banking to develop dynamically and evolve quickly—over time, business models may arise that seek to rely on the sharing and use of consumer financial services data for non-financial services sector transactions, and/or on access to non-financial services data by the financial services sector. |
| **Regulation and oversight** (see Section B) | To ensure consumers have trust and confidence in the accessing and sharing of data (subject to their consent), ASIC suggests implementing the regime under a cohesive regulatory and oversight framework.<br>ASIC considers that, in the longer term, there is merit in having an overarching economy-wide regulatory framework to allow for potential cross-sector data use. However, we acknowledge that, in the short term, there are specific drivers supporting a particular and immediate focus on establishing a regime for data access and sharing in banking.<br>If the Review considers that a regime focused on banking is appropriate, at least in the near term, ASIC is willing to play an active role in supporting the development of the regulatory and oversight framework. ASIC could also play a role in monitoring compliance with this framework, either autonomously or in conjunction with other regulators (depending on the scope and coverage of the regime).<br>In terms of the design of a banking-specific regulatory framework, there are a number of potential regulatory models the Review may wish to consider:<br>• One option is to establish a new regulatory framework through new legislation with its own conduct and enforcement provisions.<br>• Alternatively, there is the possibility for a new regulatory regime to be established by amending existing legislation and introducing new Australian financial services (AFS) licence conditions.<br>One issue that would need to be addressed with the latter approach is that entities seeking to access and use consumers' banking data may not fall within the current AFS licensing regime. Establishing a new regulatory framework through separate legislation would provide more flexibility in ensuring the framework can cover future developments and evolution of an Open Banking system.<br>The banking-specific regulatory and oversight framework should address key issues and risks, such as participation in Open Banking, consumer protection, privacy, data security, liability for unathourised transactions and consumer redress, and access to data by consumers and third party service providers. |
| **Scope and coverage for banking** (see Section C) | To allow the benefits from Open Banking to be realised, in the long term, the regime should ideally cover all authorised deposit-taking institutions (ADIs) and other financial institutions, such as non-ADI consumer credit providers.<br>However, given the large portion of the market covered by the largest firms and the costs and complexity involved in establishing the regime, it may be appropriate to focus on a subset of larger firms as an initial step while the regime is developing.<br>The regime should allow consumers and trusted third party service providers to access data in a safe and secure environment.<br>The data should include consumer data (i.e. about the financial products and services consumers have acquired and their use) and non-consumer data (i.e. from financial institutions about their financial products and services). |

# A Design of an Open Banking regime in Australia

**Key points**

Setting clear objectives for an Open Banking regime in Australia is essential to ensure there is a common understanding and to encourage buy-in from all stakeholders.

The potential benefits include better informed consumers, increased competition and innovation, and better decision making by financial institutions.

Other design considerations include consumer behavioural factors, the need for common technical standards for technology, data and security, and how the regime could be implemented.

## Objectives of an Open Banking regime

9 An important starting point in developing an Open Banking regime in Australia is to set a clear list of objectives that the regime is intended to achieve. This would help:

(a) ensure the design (e.g. the regime's scope and coverage and regulation and oversight framework) and implementation approach are consistent with and support those objectives;

(b) facilitate a common understanding among all stakeholders; and

(c) encourage buy-in from stakeholders.

10 ASIC's vision is to allow markets to fund the economy, and in turn, economic growth. In doing so, we contribute to the financial wellbeing of all Australians. One means by which we achieve our vision is through promoting trust and confidence.

11 To ensure Australian consumers can take advantage of, and benefit from, the potential new opportunities from Open Banking, the regime must be underpinned by trust and confidence.

12 As the Productivity Commission recently stated in its final report on *Data availability and use*:

> A key to achieving the many potential benefits of data use will be building and retaining community trust in how data are managed and used and building a shared understanding of the benefits that flow from better data access and use, including by consumers themselves.
>
> Note: See Productivity Commission, *Data availability and use: Overview and recommendations*, Final report, No. 82, March 2017, p. 121 (PDF, 4.69 MB).

13 Some suggested objectives for the Review's consideration include:

(a) empowering consumers to make informed financial decisions;

(b) stimulating more competition in the financial services sector;

(c) contributing to financial capability by encouraging better financial engagement among consumers;

(d) enabling consumers to share their financial services data with trusted third parties in a safe and secure manner, with appropriate consent;

(e) fostering innovation and encouraging development of new types of products and services that would benefit consumers;

(f) enabling consumers to effectively compare financial product and service offerings;

(g) enabling financial institutions and third party service providers to offer or recommend financial products and services that are individually tailored to consumers' needs; and

(h) enabling consumers to switch to another financial institution and/or third party service provider where appropriate.

## Potential benefits of Open Banking

14 ASIC envisages that Open Banking would allow consumers to access their own financial services data (i.e. data on the products and services they have acquired and data on their use of financial products and services). It would also facilitate consumers gaining access to financial institutions' data about the institutions' products and services.

15 We also envisage that third party service providers would ultimately be able to access consumers' data, where consumers have provided explicit consent. Third party service providers would include all providers other than the financial institution from which a consumer has acquired their product or service, and may include established and new financial institutions and new types of third party service providers that might emerge under Open Banking (e.g. account aggregation service providers).

16 Further, Open Banking could involve financial institutions allowing third party service providers to access data on their products and services in a standardised, machine-readable data format to enable aggregation and comparison.

> Note: For a further discussion on the types of financial institutions, data sets and third party service providers that ASIC considers could be covered under an Open Banking regime, see Section C of this submission.

17 Depending on the design of Australia's Open Banking regime, the following benefits could flow from increasing access to data.

## Better informed consumers

18 Open Banking could give consumers better access to financial services data in an aggregated, easy-to-understand format that may help them to manage their finances more effectively and empower them to make better informed financial decisions.

19 Depending on how it is designed, Open Banking could:

(a) provide consumers with more relevant information that may help them with their decision making;

(b) encourage consumers to search products and services that are available on the market; and

(c) allow consumers to compare and assess the quality and value of available financial products and services.

20 Open Banking could also facilitate the development of new types of services (e.g. choice engines and aggregation tools) that could help consumers to:

(a) better understand and manage their financial position (e.g. cash flow management and budgeting);

(b) better assess and manage risks through having an aggregated view of their personal financial positions; and

(c) more easily identify and switch to financial products and services that are more suitable to their needs and/or deliver better value for money.

21 Open Banking may also be consistent with consumer expectations. Consumers are increasingly seeking web-based information and third party reviews to inform their purchasing decisions. Consumers' reliance on these services is expected to increase over time.

22 Although consumers can currently access some data and information, this is usually in a format, and at a point in time, which inhibits consumers from benefiting from this access.

23 For example, certain post-sale data is available through annual statements and transaction and loan records, while some pre-sale data, such as product structure, fees, terms and conditions, is available through disclosure documents (e.g. Financial Services Guides and Product Disclosure Statements). However, this data is not typically provided in a form or at a time that can influence consumer decision making. It is also provided in an inconsistent format across financial institutions, which does not support aggregation and meaningful comparison.

24 It is often difficult for consumers to determine the performance of a financial product or service simply by reading the terms and conditions in a mandated disclosure document. Therefore, consumers often make decisions based on factors such as brand recognition, which encourages inertia and incumbency.

25 The financial services regime currently relies on the provision of mandated disclosure documents (which can occur before, at or even after the point of sale) to promote informed consumer decision making. In practice, the limitations of disclosure as a means of achieving this objective are well recognised and were articulated in the final report of the Murray Inquiry.

26 Therefore, in addition to providing consumers with greater access to their own data, we consider there can be a public benefit from making some private sector data publicly available, particularly in the financial services industry, due to the inherent complexity of financial products and services. In particular, key indicators derived from financial institutions' data can provide a more direct and powerful indicator of the quality or value for money of a financial product or service than a detailed comparison of a lengthy disclosure document.

27 Open Banking has the potential to help consumers make better informed decisions by enabling innovation that can give consumers relevant and targeted information at the right time. For example::

(a) patterns of past usage of products and services could inform a consumer's choice of a new product or a decision to switch to a new financial institution; and

(b) more granular and current data about the ongoing performance of a product in a variety of areas, and in a comparable format, could provide insights to help consumers assess the quality and value for money of a product.

## Increased competition and innovation

28 Competitive markets play an important role in delivering positive consumer outcomes in the financial system. Competition is a key contributor to efficient outcomes for price, quality, choice and innovation.

29 To the extent that Open Banking involves financial institutions granting third party access to data on their products and services, it has the potential to act as a catalyst for more competition and innovation in the Australian financial services industry by:

(a) providing consumers with choice, through better access to a wider set of products and services;

(b) facilitating consumers making choices by reducing the cost, time and effort required to choose or change to a different financial institution;

(c) encouraging industry to develop products and services and innovative consumer interfaces with features that are tailored to consumers' needs; and

(d) reducing barriers to entry through levelling the playing field between large incumbents and new industry entrants.

30 For example, enhancing data access by choice engines (e.g. decision making or comparison websites that have been designed responsibly) could allow consumers to more easily compare products and interpret disclosure information to help them find a product or service that best meets their needs. It could also increase competition between financial institutions by giving consumers access to greater choice, better quality and competitive prices.

### Better decision making by financial institutions

31 Open Banking may enable consumers to allow trusted third parties to use their data in ways that would assist sound decision making by financial institutions. For example, a lender's access to a prospective borrower's comprehensive banking transaction history could inform their loan approval decision.

> Note: The *National Consumer Credit Protection Act 2009* requires some lenders to obtain bank statements when complying with their responsible lending obligations.

32 Although this data can currently be shared manually, accessing it through an Open Banking platform could enable the data to be transferred more quickly in machine-readable format and provide the lender with comfort that the records are genuine and reliable.

33 Access to consumer and product data may also enable established and new financial institutions to provide tailored advice to consumers about potentially suitable products and services.

## Other design considerations

### Consumer behavioural factors

34 For consumers to realise the benefits noted above, it is critical that the design and implementation of the Open Banking regime be informed by an understanding of consumer behavioural factors, including behavioural biases, and how they can impede good consumer outcomes from financial products and services.

35 Research shows that different biases can be triggered depending on how information is presented. Developing research also shows that these biases can be amplified in a digital environment.

> Note: Benartzi, S. and Lehrer, J., *The smarter screen: What your business can learn from the way consumers think online,* 2015, Piatkus, London, p. 31. For a further discussion on consumer behavioural factors, including behavioural biases, and how they affect consumer decision making, see Appendix 1 of this submission.

36 The unique ways in which consumers can interact with information across different mediums demonstrate the importance of designing an Open Banking regime which incorporates behavioural insights. Rather than trying

to adapt the traditional disclosure framework (with its acknowledged limitations), the introduction of an Open Banking regime provides an opportunity to develop a new and tailored approach to facilitating consumer engagement with, and understanding of, data and information.

37 Although access to data may be enhanced under Open Banking, it does not automatically mean that consumers will engage with it, understand how or why it should be used, or act on the data when making decisions.

38 A number of factors are likely to contribute to whether data provided through an Open Banking regime positively influences consumer decision making, including:

(a) whether the provider or comparator is trusted and trustworthy;

(b) that the framing and structure of the information accounts for (and does not seek to exploit) behavioural biases associated with decision-making about financial services and products (e.g. burying important features, providing unrepresentative or incomplete comparison lists);

(c) the timeliness of data provision in relation to decision making;

(d) whether consumers understand how the data should be incorporated into their decision-making; and

(e) whether the platform through which the data is accessed (and the data itself) is structured in a consumer-centric manner (i.e. easy to find, navigate).

39 Accordingly, consumer testing and collecting and analysing relevant data to measure outcomes should be considered when developing the design of the Open Banking regime. This can help avoid relying on assumptions about how consumers and firms are likely to behave in response to the introduction of the regime.

40 Example 1 discusses some findings based on consumer policy development in the United Kingdom.

**Example 1: The impact of annual summaries, text alerts and mobile apps on consumer banking behaviour (UK experience)**

In the United Kingdom, the Financial Conduct Authority (FCA) found that annual summaries had no effect on consumer behaviour in terms of incurring overdraft charges, altering balance levels or switching to other current account providers.

In contrast, signing up to both text alerts and mobile banking apps resulted in a 24% decrease in the number of unarranged overdraft charges.

This example shows the benefits of consumers receiving information just in time (without having to actively acquire it), as well as being able to act quickly upon receiving the information (via the banking app).

Note: FCA, *Message received? The impact of annual summaries, test alerts and mobile apps on consumer banking behaviour*, Occasional Paper No. 10, March 2015.

## Technical standards for technology, data and security

41 To facilitate broad participation in Open Banking, we think there is a role for common standards that define specific data sets that need to be shared, how data should be created, stored and shared, and how data should be accessed.

42 The adoption of common technical standards for technology, data and security may support implementation by providing more certainty to industry, facilitating collaboration and ensuring interoperability (i.e. via same messaging and interface standards). This is supported by international experience: see Example 2.

**Example 2: Implementation of common technical standards (UK/EU experience)**

In the United Kingdom, an independent implementation entity has been appointed to drive the development of common standards and support implementation.

In addition, common standards have been adopted for sharing access to data, such as open Application Programming Interfaces (APIs). For security and communication, OAuth 2.0 and OpenID Connect (OIDC) have been adopted as the authentication and authorisation standards for open APIs. Open APIs also need to be made available under an 'open' licence so they can be freely used, reused and distributed.

The UK approach to technical standards is considered to be more interoperable and supportive of innovation compared to other implementation approaches across the European Union.

In the European Union, there is some industry concern that the lack of common standards will lead to the development of an over-abundance of APIs and result in unnecessary duplication and costs, including possibly diluting the benefits from opening the banking system.

Note: Banking Tech, *Open banking APIs will require a rulebook to ensure 'good outcome*', 15 July 2016.

## Implementation

43 To enable timely implementation, minimise the burden on industry and build consumer trust, ASIC agrees with the Review's suggestion to consider a phased introduction of the regime. We also agree that it would be prudent to learn from the initial operation of Open Banking in other jurisdictions.

# B Regulation and oversight

**Key points**

In this section, we look at different options for developing a regulatory model to ensure that an Open Banking regime in Australia delivers the desired objectives and outcomes.

We also consider the key risks and issues that could arise under Open Banking and how these could be addressed through regulation and oversight.

## A cohesive framework for regulation and oversight

44 To ensure consumers have trust and confidence in the regime, and are willing and able to take advantage of the opportunities Open Banking offers, ASIC suggests implementing the regime under a cohesive regulatory and oversight framework.

45 This framework should address elements such as coverage of all Open Banking participants, privacy, the security of data, liability for unauthorised transactions, redress for consumers, and access to data by consumers and third party service providers.

46 Ultimately, consumers' experience with how their data is treated is a critical issue for businesses. How businesses manage and protect privacy and data use will likely become an important measure of the level of consumer trust and confidence in businesses. If consumers no longer trust the businesses they are dealing with, this trust will be difficult to regain and will impact the long-term sustainability of those businesses. In this context, it could also impact on consumers' trust and confidence in Open Banking.

47 In this environment, the financial services sector will need to create a culture of ethical and responsible use of data—this could require industry to go above and beyond any minimum standards set in the Open Banking regulatory and oversight framework.

## Developing a regulatory model

48 The regulatory model chosen for Open Banking will ultimately depend on what the regime is intended to achieve and its design. For this reason, we consider that setting objectives and outcomes for introducing Open Banking in Australia is an essential starting point.

49 While ASIC supports industry co-regulation (e.g. industry develops and administers its own arrangement and government provides legislative

backing to enable the arrangements to be enforced), this approach is only appropriate under certain circumstances. For example, industry does not always have the incentives to develop strong and cohesive standards and allocate obligations and liabilities between participants.

> Note: See, for example, Commonwealth of Australia, Taskforce on Industry Self-regulation, *Industry self-regulation in consumer markets*, August 2000 (PDF, 527 KB).

50 Open Banking could potentially develop to involve a diverse and fragmented group of industry players and the potential risks for loss of consumer trust and confidence could be significant if things go wrong (e.g. financial loss and/or loss of privacy). For these reasons, ASIC considers that a government-led approach for the regulation and oversight of the Open Banking regime is warranted.

> Note: See Appendix 2 of this submission for more information on the advantages and disadvantages of co-regulation versus government regulation.

51 This approach would be consistent with the Productivity Commission's recommendations on the implementation of a new, broad framework for data in Australia that is underpinned by legislation.

> Note: See Productivity Commission, *Data availability and use: Overview and recommendations*, Final report, No. 82, March 2017 (PDF, 4.69 MB).

## Potential regulatory models

52 ASIC considers that, in the longer term, there is merit in having an overarching economy-wide regulatory framework to cover data access and sharing. While this approach would provide consistency, there may be a need for scalability and appropriate variations given the different sensitivities and risks of particular types of data. For example, consumers' financial services data may have greater sensitivity than some other types of consumer data. Sharing of financial services data also raises risks of financial loss arising from unauthorised use.

53 Given the pace of change and innovation, it also seems likely that, overtime, there may be a need for cross-sector use. Business models may develop that seek to rely on access to consumers' financial services data for transactions outside financial services or to consumers' non-financial services data within the financial services context. In that environment, there are likely to be benefits in having an overarching economy-wide regulatory framework.

54 However, ASIC acknowledges that there are specific drivers requiring a particular and immediate focus on establishing a regime for data access and sharing in banking. These drivers include the volume and importance of data in banking, the centrality of data for consumer and service provider decision making for banking transactions, the current growth and innovation in the fintech sector, and the goal of promoting competition in banking.

55 Therefore, in the shorter term, there may be a need to establish a banking-specific regulatory framework. In establishing such a framework, it would be appropriate to consider the potential for the Open Banking framework to form part of an overall economy-wide regulatory framework in the medium to longer term (depending on broader developments in the economy and subsequent policy decisions).

56 If the Review considers that, at least in the near term, a regime focused on banking is appropriate, ASIC is willing to play an active role in supporting the development of the regulatory and oversight framework. We could also play a role in monitoring compliance with this framework, either autonomously or in conjunction with other regulators, depending on the scope and coverage of the regime.

## A banking-specific regulatory framework

57 In terms of the design of a banking-specific regulatory framework, there are a number of potential regulatory models the Review may wish to consider.

58 One option is to establish a new regulatory framework through new legislation with its own conduct and enforcement provisions. The new legislation could incorporate principles from existing privacy legislation and financial services legislation such as the *Corporations Act 2001* (Corporations Act), but include new requirements around consumer rights and protections.

59 Alternatively, as suggested in the Review's Issues Paper, there is the possibility for a new regulatory regime to be established by amending existing legislation and introducing new AFS licence conditions.

60 One issue that would need to be addressed is that entities seeking to access and use consumers' banking data may not fall within the current AFS licensing regime. Businesses that do not provide a service to consumers that falls within the statutory definition of 'financial service' are not required to hold an AFS licence.

61 Currently fintech start-ups that provide aggregated transaction account data (by using 'screen scraping' techniques that rely on the consumer (i.e. the holder of the bank account) first inputting their internet banking login and password) are not required to hold an AFS licence. This is because merely providing factual information (i.e. transaction account data) is not financial advice unless it involves the expression of an opinion or recommendation intended to influence a client in making a decision about a particular financial product.

62 Assuming an entity accessing consumers' banking data was providing a financial service, there may be scope for making regulations to prescribe conditions on an AFS licence (e.g. s914A(8)), or to prescribe further general conduct obligations (e.g. s912A(1)(j)) or to prescribe other requirements that must be met before a licence can be granted (e.g. s913B(1)(d)). However, ASIC's powers to enforce AFS licensing requirements are limited to administrative actions rather than the full range of penalties.

63 Another consideration is whether establishing a new regulatory framework through new legislation would provide more flexibility to ensure it:

(a) can cover all potential users of banking data, including various functionally similar products (e.g. transaction accounts, stored value cards or credit cards)—noting that it would be important to analyse any potential regulatory risks raised by particular types of products;

(b) is sufficiently technology-neutral to accommodate innovations and technologies that are yet to emerge; and

(c) is adaptable so it can accommodate ongoing developments and the evolution of an Open Banking system.

## Suggested elements for a regulatory and oversight framework

64 Table 2 summarises ASIC's views on suggested elements for addressing the risks and issues under an Open Banking regime.

**Table 2: Suggested elements to address key risks and issues of an Open Banking regime**

| Key risks and issues | How they could be addressed |
|---|---|
| **Participation in Open Banking** (see paragraphs 65–69) | • Design of the regulatory and oversight framework |
| **Consumer protection** (see paragraphs 70–74) | • Consumer rights to data |
| **Privacy** (see paragraphs 75–89) | • Consumer consent and privacy notices<br>• Process for seeking consent |
| **Security** (see paragraphs 90–102) | • Requirements relating to management of operational and security risks<br>• Authentication requirements<br>• Rights and responsibilities in the event of an incident |
| **Liability and consumer redress** (see paragraphs 103–113) | • Allocation of responsibilities and liabilities<br>• Consumer rights, including rights to compensation and remedies<br>• Providers' capacity to repay<br>• Dispute resolution framework |

| Key risks and issues | How they could be addressed |
|---|---|
| **Governance and accountability** (see paragraphs 114–117) | • Requirement to demonstrate organisational/operational measures for meeting regulatory obligations, accompanied by regulatory oversight mechanisms |
| **Access to data** (see paragraphs 118–124) | • Mandate for data sharing |

## Participation in Open Banking

65 A key issue to address is that all participants of Open Banking should be subject to a cohesive regulatory and oversight framework.

66 This is essential in ensuring:

(a) established and new financial institutions and new types of third party service providers, that are not currently required to be licensed under the existing financial services regulatory regime, are covered;

(b) the relationship between consumers, financial institutions and third party service providers can be clearly defined;

(c) rights, responsibilities and obligations relating to privacy, data security, liability, consumer redress, accountability and governance, and access to data can be clearly identified;

(d) conduct and enforcement provisions are clearly set out; and

(e) consumers have confidence that all parties they are dealing with under an Open Banking regime are subject to a regulatory and oversight framework.

67 Example 3 outlines the approach taken in the United Kingdom to a regulatory and oversight framework for Open Banking participants.

**Example 3: Regulatory framework for licensing Open Banking participants (UK experience)**

The first European Payment Services Directive (PSD) was implemented in the United Kingdom through the Payments Services Regulations in 2009. This established a European-wide legal framework for payment services by setting the information requirements and the respective rights and obligations of payment service users and providers.

This framework distinguishes between six categories of participating service providers (PSPs), including credit institutions, electronic money institutions, post office giro and payment institutions. ‘Payment institutions’ are providers of payment services that are not connected to the taking of deposits or the issuing of electronic money.

The revised Payment Services Directive (PSD2) introduces two new types of payment services:

**Example 3 (cont.)**

- A 'payment initiation service' (PIS) is defined as a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider.
- An 'account information service'(AIS) is defined as an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider.

'Payment initiation service providers' (PISPs) and 'account information service providers' (AISPs) are generally collectively referred to as third party providers. Consumers have a right to use PIS and AIS where the payment account is accessible online and where they have given explicit consent.

PSD2 also introduces another new definition, 'account servicing payment service provider' (AS PSP), to distinguish the provider where the consumer's payment account is held.

Payment institutions need to be authorised to offer payment services by fulfilling various requirements. The Financial Conduct Authority (FCA) is responsible for authorisation of payment institutions in the United Kingdom. Any PSP, subject to having the appropriate authorisation, including an AS PSP, could potentially offer PIS or AIS.

PSD2 defines a lighter prudential regime for AISPs, which are treated as payment institutions but are only subject to some of the provisions about transparency, information, rights and obligations. The European Banking Authority (EBA) is obliged to develop, operate and maintain a publicly available electronic central register containing information drawn from the public registers in each European Union Member State, identifying the payment services for which each payment institution is authorised or for which an AISP is registered.

Note: On 12 January 2018, PSD2 will be transposed into national law in the United Kingdom and most articles will apply from that date with a few exceptions (e.g. the EBA's Regulatory Technical Standards on strong customer authentication and common secure communication will run to a different implementation schedule and will apply 18 months after PSD2 comes into effect).

68 This approach is preferable to the approach in the United States, where we understand large banks are striking data sharing deals with individual partners.

Note: See Brodsky, L. and Oakes L., *Our insights: Data sharing and open banking*, McKinsey and Company, September 2017.

69 An approach that relies primarily on contractual relationships between participants for ensuring accountability is not the most appropriate model for supporting the key objectives and outcomes of an Open Banking regime in Australia, particularly the suggested objectives in Section A, or the suggested elements in Table 2 for a regulatory and oversight framework in addressing key risks and issues.

## Consumer protection

70 To ensure consumer protection, consumers need to have specific rights to determine who can access their data and what they can do with it.

71 ASIC regards the five elements of the Productivity Commission's proposed comprehensive right to data as a useful starting point. As proposed, the right would enable consumers to control their data through:

(a) requesting edits;

(b) receiving a copy of the data;

(c) directing data to be transferred;

(d) being advised if data is traded; and

(e) being informed of data disclosure.

72 We note that the recent revision to the European General Data Protection Regulation (GDPR) includes new consumer rights to 'data erasure' and 'data portability' and rights for 'consumers to object at any time to the processing of their data'.

Note: These requirements will apply from 25 May 2018.

73 ASIC understands that the Productivity Commission considered and made a decision not to adopt the additional rights under the GDPR. However, consumer financial services data is more sensitive relative to some other types of consumer data and there are significant consequences from a privacy breach of this data. Accordingly, it might be worthwhile for the Review to consider whether the additional rights under the GDPR would be beneficial in enhancing consumer privacy protections, and whether it justifies revisiting this issue in the context of Open Banking.

74 Another issue is the potential for new sales, distribution and pricing practices to emerge under an Open Banking regime, which may result in reduced access for certain consumers. For example, new pricing practices may be developed based on more detailed segmentation of consumer risk or other characteristics as a result of increased access to consumer data. Giving consumers comprehensive rights to their data, as recommended by the Productivity Commission, may address these issues.

## Privacy

75 Open Banking involves significant privacy implications. Consumers need to be confident that their data cannot be accessed inappropriately or used without their permission to have trust and confidence in the regime.

76 Mechanisms for managing and protecting privacy will be critical to ensuring confidentiality and integrity of consumer data. This includes ensuring consumer consent is sought, recorded and kept up to date, and appropriate systems and controls are in place to ensure only those who have been granted permission are able to access data.

### Consumer consent and privacy notices

77 Another mechanism for consumer protection is to introduce a mandatory requirement that third party service providers seek explicit consumer consent. We consider it would be worthwhile exploring whether different types of consent should apply depending on the type of permission being granted (e.g. ability to view consumers' transaction data; ability to process payments on behalf of consumers), and whether ongoing and one-off consent should be allowed, depending on the nature of permission being granted.

78 The revised PSD2 mandates explicit consent in two ways:

(a) Third party access to consumer data must be given only at the explicit consent of the customer.

(b) Data should not be used, accessed or stored for any purpose other than the service the user explicitly requested.

79 Under PSD2, consumers and businesses may grant permission to an AIS to allow it to obtain a consolidated view of their accounts and to use tools to analyse their transactions and spending patterns with one or more AS PSPs. This could be on an ongoing basis where there is a long term relationship between the consumer and the AISP. Alternatively, consent could be given for one-off access in order to enable, for example, an affordability check to be carried out when applying for a loan.

80 The GDPR includes a new definition of consent. It states that consent must be freely given, specific, informed and unambiguous. Consent is not freely given if the individual has no genuine or free choice or is unable to refuse or withdraw consent at any time.

81 The GDPR also requires businesses to make the withdrawal of consent as easy as giving consent, and, before individuals give consent, must inform individuals about this right to withdraw consent. In addition, individuals must be provided with a range of prescribed information about the processing of their personal data.

82 We note that the *Privacy Act 1988* (Privacy Act) and GDPR have common requirements:

(a) The four key elements of consent are that the individual is adequately informed before giving consent, the individual gives consent voluntarily, the consent is current and specific, and the individual has capacity to understand and communicate consent.

(b) The Privacy Act also requires entities that collect personal information to take reasonable steps to give individuals notice about certain matters.

### Process for seeking consent

83 The process for obtaining consumer consent is critical so that consumers are aware of the permission they are granting. We suggest the Review consider measures to ensure transparency in the consent process and the use of personal data (including the potential for on-selling of data).

84 Although privacy regulation is based mostly around consent, we are aware that consent is often not made in an informed or meaningful way:

(a) Consumers may experience difficulty in fully understanding the implications of providing access to their personal data; therefore, they may not be able to make an informed judgement about granting access.

(b) A common process for seeking consent is where a box associated with a long list of terms and conditions is requested to be ticked.

85 Accordingly, there may be a role for consumer testing in designing the point of consent to ensure consumer understanding.

86 Our work in researching behavioural insights also suggest that even if consumers are aware of their rights, they may not make choices that reflect their preferences. This is because choices are frequently influenced by behavioural biases and the decision context, including the choice environment.

87 While disclosure is one potential mechanism for improving consumer awareness, disclosure should not be regarded as an end in itself— since it is not always effective in influencing behaviour.

88 There may be a role for tempering consumer responsibility, and introducing additional protections, in circumstances where it is not reasonable to expect consumers to understand or foresee the consequences of making a particular decision in relation to their data (e.g. rights to be informed about the financial institution's intention to disclose or sell data to third parties, and avenues for redress and remedies: see paragraphs 103–113).

89 Ultimately, the standard of consent should depend on the potential consumer harm from proposed use of the data. Depending on the situation, this could be general consent as part of the terms of using the relevant product or service, or may need to be more specific consent for particular types of data.

## Security

90 Because Open Banking would increase the flow of data between consumers, financial institutions and third party service providers, data security will be a significant issue—specifically, how data can be collected, stored and shared securely. Enabling consumers to share data could increase the risk of fraud, the illegal use of sensitive and personal data, other abuses such as imitation services, and cyber threats.

91 For these reasons, the regulatory and oversight framework should include requirements around transparency (i.e. what information is being collected, what it will be used for and how it will be shared).

92 The framework should also include requirements for systems and controls to ensure data cannot be used, accessed or stored for any purpose other than the purpose explicitly granted by the consumer. This includes requirements for managing operational and security risks by Open Banking participants, requirements for ensuring strong consumer authentication, and requirements on rights and responsibilities in the event of a data breach.

### Management of operational and security risks

93 Financial institutions and third party service providers should have a clear understanding about their responsibilities when managing, sharing and using data. This may be achieved through introducing mandatory requirements for managing operational and security risks, including system performance monitoring, contingency measures for unplanned unavailability or a systems breakdown, and incident management and reporting.

94 Such requirements have been introduced under PSD2:

(a) All PSPs are required to establish a framework for managing operational and security risks, including setting up and maintaining incident management procedures to include the detection and classification of major operational and security incidents.

(b) PSPs are required to monitor the performance of their Application Programming Interface (API) and include a strategy and plans for contingency measures in the event of an unplanned unavailability of the API and systems breakdown.

(c) In the event of a major operational or security incident, all parties must notify their regulator without delay. Incident reports are required to be updated every three days and a full report with root cause analysis is required within two weeks of a business being back to normal. Should the incident impact on the financial interests of consumers, the PSP will also be required to inform the consumer without undue delay and advise them of measures to mitigate any adverse consequences.

(d) At least annually, PSP are required to provide specific reporting to their regulator, including regarding updated operational and security risk assessments, the adequacy of the control and mitigation measures deployed and statistical data on fraud.

### Authentication

95 There is a need for consumer protections against fraud and possible abuses.

96 Strong customer authentication for electronic payments has been mandated under PSD2 to protect the confidentiality and integrity of consumers' personalised security credentials. Specifically, PSPs are required to use strong customer authentication when a payer accesses their payment account online, initiates an electronic payment transaction and carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.

97 The EBA's Regulatory Technical Standards for strong customer authentication and secure communication, which form the backbone of PSD2, also set out how the various parties will interact with each other. For example, consumers must be securely authenticated (two factors) for virtually all transactions (except a few low-value exemptions) on a channel or device different from the one that initiated the payment.

98 Third party service providers such as retailers and account aggregators must become 'identity enabled' to participate. The Regulatory Technical Standards also suggest that risk factors (e.g. location, transaction history and spending patterns) should be monitored and factored into authentication and authorisation decisions.

99 PISPs and AISPs can rely on the authentication procedures provided by the AS PSP to the consumer. However, they must ensure that the personalised security credentials are not shared with other parties, they must not store sensitive payment data, and they are obliged to identify themselves to the AS PSP each time a payment is initiated or data is exchanged.

### Responsibilities in the event of a data breach

100 The regulatory and oversight framework should also clearly outline the responsibilities of financial institutions and third party service providers in the event of a data breach. This includes clear rules around the nature of data breaches that are required to be reported, to whom the breach should be reported and the timeframe for notification.

101 Under the GDPR, data controllers must advise their regulator of a data breach within 72 hours of becoming aware of the breach. Data processors must notify the controller of a breach without undue delay. In addition, when a data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller must notify the individual without undue delay.

> Note: Data controllers determine how and why personal data is processed. Data processors act on behalf of the controller.

102 While data breach notification is not universally mandatory in Australia, it is considered good privacy practice. The Office of the Australian Information Commissioner (OAIC) has published *Data breach notification—A guide to handling personal information security breaches* (August 2014) to provide general guidance for agencies and organisation when responding to a data breach involving personal information they hold. This s complemented by the OAIC's *Guide to developing a data breach response plan* (April 2016).

Note: The *Privacy Amendment (Notifiable Data Breaches) Act 2017*, which commences in February 2018, will apply to organisations and agencies that are subject to the Privacy Act.

## Liability and consumer redress

103 To ensure trust and confidence in Open Banking, financial institutions and third party service providers need to have a clear understanding of their responsibilities and obligations. Consumers also need to know their rights, including rights to compensation and remedies.

104 One important issue is the allocation of liabilities and consumer rights in the event of an unauthorised, non-executed or delayed payment.

105 The ePayment Code regulates consumer electronic payments, including ATM, EFTPOS and credit card transactions, online payments, internet and mobile banking and BPAY. The Code is currently a voluntary code of conduct and has approximately 120 subscribers (including most Australian ADIs and other providers of electronic payment facilities). Among other things, the Code sets the rules for determining who is liable for unauthorised transactions. Compliance with the Code is a required term of the contract between the subscriber and each account or facility holder.

106 The Final Report of the Financial System Inquiry recommended that the Code be made mandatory. Government has supported this recommendation. The process of mandating the Code is currently progressing.

107 Under PSD2, the provision of PIS and AIS is not dependent upon the existence of a contractual relationship between the third party provider and the AS PSP. In terms of the liability regime, in the event of an unauthorised, non-executed, defective or late executed payment initiated via a PISP, the AS PSP is required to refund the customer immediately. The PISP has an obligation to immediately compensate the AS PSP. The PISP needs to prove that the payment was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency to its payment service.

108 PSD2 also includes specific consumer rights:

(a) The amount a payer could be obliged to pay in the event of an unauthorised payment is €50, except in cases of fraud or gross negligence by the payer.

(b) Consumers have an unconditional refund right (for a period of 8 weeks from the date when the funds were debited).

109 Clarity about dispute resolution, and the extent of coverage, is also essential. Consumers will need assurance that if things go wrong, they can take their dispute to an appropriate dispute resolution scheme

110 Given the number of parties that are likely be involved in a dispute under Open Banking, there is a risk that a third party service provider (or other third party in the transaction with whom a consumer does not have a trusted or direct relationship) may not be a member of an existing EDR scheme. Open Banking could potentially encompass new start-ups and emerging businesses providing services. These providers may also not be part of an existing EDR scheme and/or have sufficient capital to indemnify a consumer for their losses. The nature of data security breaches is such that one event may impact a large number of consumers and potentially raise numerous claims for compensation if the compromised data is misused.

111 To avoid gaps in a consumer's ability to access remedies, the regulatory and oversight framework should include specific requirements for dispute resolution.

112 For example, under PSD2, PSPs must have in place dispute resolution procedures and respond to payment complaints within 15 business days of receipt. Third party PSPs also have to meet certain capital requirements and hold professional indemnity insurance. In addition, the FCA in the United Kingdom is required to monitor compliance with PSD2 and the Financial Ombudsman is required to handle disputes between payment service providers and consumers.

113 Depending on the scope and coverage of the Open Banking regime, the dispute resolution framework could be incorporated into the existing financial services dispute resolution framework. Alternatively, a new body could be established. Since a broad range of participants are likely to be involved in the Open Banking regime and some newer entrants may have more limited capital, it may also be worth considering whether other mechanisms should be in place for ensuring that entities responsible for a breach will be able to compensate consumers.

## Governance and accountability

114 To ensure Open Banking participants comply with their obligations, the framework should also include specific organisational/operational governance and accountability requirements for financial institutions and third party service providers and an oversight mechanism for regulator(s).

115 For example, under the GDPR, data controllers must:

(a) comply with 'Principles relating to the processing of personal data' (this is referred to as the 'accountability principle');

(b) ensure and demonstrate through the implementation of appropriate technical and organisational measures, including data protection policies, that their processing activities comply with the GDPR;

(c) implement technical and organisational measures to show that they have considered and integrated data protection into their processing activities (this is referred to as 'data protection by design and by default');

(d) appoint data protection officers to monitor and advise on compliance with the GDPR and with internal privacy policies and procedures; and

(e) undertake a compulsory data protection impact assessment prior to data processing, where a type of processing is likely to result in a high risk for the rights and freedoms of individuals.

116 The GDPR obligations in subparagraphs 115(a)–115(c) are similar to Australian Privacy Principle (APP) 1.2, which requires APP entities to:

> take reasonable steps to implement practices, procedures and systems to ensure compliance with the APPs (and any applicable registered APP code) and to enable complaints.

117 Other jurisdictions use various oversight mechansims. One approach is to require financial institutions and third party service providers to submit an independent audit report to the regulator periodically. Another involves financial institutions and third party service providers undertaking an annual self-assessment (with a prescribed set of criteria and a report to the regulator to demonstrate how they have complied, and will continue to comply, with their obligations), with the regulator undertaking periodic surveillances on financial institutions and third party providers. For example, under PSD2, PSPs are required to provide specific annual reporting to their regulator about the adequacy of their security control and mitigation measures.

## Access to data

118 An Open Banking regime may not be in the commercial interests of all existing financial institutions, especially where the data they hold provides them with a proprietary advantage over new entrants.

119 Since existing financial institutions may lack incentives to release data (i.e. consumers' data and financial institutions' own data on their products and services), we suggest the Review consider whether there is a role for regulation to facilitate or mandate data sharing.

120 Good access to data by third party service providers, on a timely basis, is critical to the success of an Open Banking regime. It is important that, subject to consumers' consent, all third party service providers have equal access to a pre-defined set of data.

121 The experience in other jurisdictions suggests that in the absence of a mandatory requirement being introduced it is unlikely that existing financial institutions will provide access to data voluntarily or provide access without imposing restrictions or charging fees–which act as barriers to competition.

122 Data is a valuable resource. By keeping it proprietary, existing financial institutions can retain a competitive advantage over fintechs. For existing financial institutions, allowing access to data in a safe and secure manner will likely involve significant IT spend while potentially eroding their market share and profitability.

123 A mandate requiring financial institutions to share data securely may help accelerate digital change, enable new types of services to be developed to provide better consumer choice and increase competitiveness across the entire sector.

124 We understand that a decision has been made in the United Kingdom to drive the implementation and adoption of Open Banking by introducing a mandate to ensure the nine largest UK banks will share their data securely with other banks and third parties. We also understand that the voluntary approach adopted by Singapore has had limited success in encouraging financial institutions to adopt Open Banking.

# C Scope and coverage for banking

**Key points**

This section outlines the types of financial institutions, data sets and third party service providers that ASIC considers could be covered under an Open Banking regime.

We anticipate that the potential gains from Open Banking in Australia will increase as consumers and, with consumer consent, third party service providers, obtain access to larger amounts of relevant data.

## Types of financial institutions

125 To allow the benefits from Open Banking to be realised, in the long term, the regime should ideally cover all ADIs and other financial institutions, such as non-ADI consumer credit providers. However, given the large portion of the market covered by the largest firms, and the costs and complexity involved in establishing the regime, it may be appropriate to focus on the subset of larger firms as an initial step while the regime is developing.

126 Covering all ADIs would ensure all consumers can benefit from being able to access their data. It would also ensure consumers who have financial dealings with more than one financial institution would be able to obtain an aggregated view of the data for all their accounts.

127 All credit providers would also benefit from being able to view aggregated consumer data to support their responsible lending assessments and risk management processes (e.g. fraud identification and management). For example, lenders would be able to access a prospective borrower's transaction history, regardless of which ADI(s) the borrower banked with.

128 Although, in the longer term, it would be useful for the Open Banking regime to cover all ADIs and other financial institutions, a comprehensive regulatory impact assessment would allow the costs and benefits to be fully assessed. This would include evaluating the costs and benefits based on the size of financial institutions, as the implementation costs would likely have a greater impact on smaller participants due to economies of scale.

## Types of data sets

129 As discussed in Section A, we consider there is merit in increasing access to the following two data sets:

(a) *Consumer data*—This includes data about financial products and services consumers have acquired and their use of these products and services: see paragraphs 132–133.

(b) *Non-consumer data*—This includes data from financial services providers about their financial products and services: see paragraphs 134–136.

130 In light of the pace of innovation in this area, it is difficult to predict all of the ways in which consumer data might be used and how this may ultimately benefit consumers. In ASIC's view, it would be beneficial for the scope of the regime to be appropriately flexible and expansive (with adequate regulatory oversight and consumer protections).

131 However, we also consider there is some data that should be out of scope in an Open Banking regime: see paragraph 138.

### Consumer data

132 Consumer data relates to consumers' transaction and loan accounts. Some examples include the following:

(a) *Bank account data*—This may include account name, number and type, BSB, account balance, interest rate, fees, interest earned, fees charged, and details of transactions (e.g. date, dollar amount and description).

(b) *Credit card data*—This may include account name, number and type, BSB, credit limit, card balance, available credit, interest rate, fees, interest-free period, interest and fees charged, balance due, minimum payment due and due date, and details for processed transactions and pending transactions (e.g. date, dollar amount and description).

(c) *Loan data*—This may include type of loan (e.g. home, car, personal), account name, number and type, BSB, credit limit, loan balance, loan repayments, interest rate and fees, interest and fees charged, amount paid in advance, loan term, fixed/variable interest rate, loan maturity date, payment frequency and next scheduled payment date.

133 Although consumers' credit repayment history data is currently accessible under the comprehensive credit reporting (CCR) regime, this framework is voluntary. The Government has indicated its support for mandating participation in the CCR regime. ASIC's view is that decisions about whether to include CCR data within the scope of Open Banking should be dependent on lender participation and broader decisions on the mandating of CCR.

### Non-consumer data

134 As discussed in Section A, we consider that one of the potential benefits from Open Banking is facilitating more consumer choice by providing access to a wider set of products and services and reducing the cost, time and effort required to change financial institutions; in turn, increasing demand-driven competitive pressure and stimulating innovation.

135 Beyond providing access to data that is personal to the consumer, there may be significant benefit in providing access to data on financial products and services available in the market, in a way that would benefit consumers (e.g. data on product features, performance and establishment and ongoing fees). ASIC is working on a number of initiatives in this area, including life insurance claims outcomes data and internal dispute resolution data.

136 Consumers may also benefit from gaining access to other general data, such as bank branch locations, trading hours etc.

### Other data

137 As a future consideration, it may also be worthwhile for the Review to explore whether Open Banking should cover data about consumers' insurance, superannuation and investments products—if not initially, then during a latter phase of a staged implementation of Open Banking.

### Out-of-scope data

138 ASIC envisages that not all data could and should be shared via Open Banking. For example, we consider data that is value-added (e.g. financial advice data and data derived from analysis of transaction data) should be out of scope.

## Third party service providers

139 ASIC envisages that Open Banking would facilitate the emergence of new types of third party services that would benefit consumers.

140 In general, third party service providers do not hold a consumer's account. This could include established financial institutions and new entrants who need access to consumers' and financial institutions' data to be able to provide their services (e.g. accounting software, online personal financial management tools allowing consumers to analyse their transactions and spending patterns with one or more financial institutions, comparison websites, account aggregation tools, and other innovative services that have yet to emerge).

141 An issue that ASIC raised in our 2016 submission to the Productivity Commission's Issues Paper on *Data availability and use* relates to 'account aggregators'. In particular, we observed that there is a degree of uncertainty among consumers and industry about how liability provisions in the ePayments Code relating to account aggregators should be interpreted.

> Note: Account aggregators can provide a range of useful services from personal financial management tools and bank statement retrieval services for lenders to other services that rely on access to a consumer's banking account to provide a range of innovative services.

142 We understand that many account aggregators in the market are using 'screen scraping' techniques that rely on the consumer (the holder of the bank account) first inputting their internet banking login and password.

143 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.

144 In ASIC's submission, we noted that, provided any data security concerns can be addressed, consumers should not be disadvantaged by their use of legitimate account aggregation services.

145 Open Banking may provide a means for consumers to safely enable trusted third parties to access their data, which may address some of the current uncertainty relating to account aggregation services and the inputting of internet banking credentials.

# Appendix 1: Consumer behavioural factors

146 For consumers to realise the benefits under Open Banking, it is critical that the design and implementation of the Open Banking regime be informed by what we know about human behaviour and the way consumers interact with information and financial products and services.

147 A significant body of work by policy makers, academics and regulators has been built over recent years from a range of social and behavioural sciences. This work describes how and why people think and behave in certain ways—that is, how they *actually* behave. 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.

148 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. They are also relevant because they can contribute to a significant weakening of the demand-side pressures that are key to driving competition.

149 Behavioural factors, which include behavioural biases, can create barriers for consumers and investors being able to access and assess information, and make decisions about financial products and services in ways assumed by traditional economic models, which can impede good outcomes. The presence of behavioural factors can also provide clear opportunities for firms to engage in conduct which exploits these biases through sales practices, framing of product information, and product structures.

> Note: A behavioural bias is a systematic tendency, inclination or opinion in relation to someone or something. They are often observed as shortcuts in our decision making. Everyone has a set of biases. They may be conscious or unconscious because we are usually not aware when we move between our instinctive and 'deeper' styles of thinking. Biases are shaped by long-term effects (such as culture, previous experiences and personal tastes) and short-term effects (such as the amount of available information or even the time of day).

150 Research also shows that different biases can be triggered depending on how information is presented. These biases can be amplified in a digital environment by:

(a) the channel through which information is provided;

(b) the timing of when the information is received in a decision process;

(c) the messenger providing the information;

(d) the format of the information; and

(e) the order in which information is presented.

151 Biases can also result in people making different choices when presented with information in a digital environment than they would when presented with the same information on paper or in person. Developing research shows, for example, people can spend less time reading information, and recall less of the information they have read, on smaller digital devices (compared to a computer screen).

> Note: Benartzi, S. and Lehrer, J., *The smarter screen: What your business can learn from the way consumers think online*, 2015, Piatkus, London, p. 31.

152 The unique ways in which consumers can interact with information across different mediums makes clear the importance of designing an Open Banking regime which incorporates these behavioural insights. Rather than trying to adapt the traditional disclosure framework (with its acknowledged limitations), the introduction of an Open Banking regime provides an opportunity to develop a new and tailored approach to facilitating consumer engagement with, and understanding of, data/information to encourage the realisation of intended consumer benefits.

# Appendix 2: Benefits and limitations of co-regulation

## What is 'co-regulation'?

153 Co-regulation generally involves both industry and regulators developing, administering and enforcing a solution, typically underpinned by legislative backing. The Office of Best Practice Regulation's *Best practice regulation handbook* states that:

> "Co-regulation" typically refers to the situation where industry develops and administers its own arrangements, but government provides legislative backing to enable the arrangements to be enforced. This is often referred to as 'underpinning' of codes, standards and so on. Sometimes legislation sets out mandatory government standards, but provides that compliance with an industry code can be deemed to comply with those standards. Legislation may also provide for government-imposed arrangements in the event that industry does not meet its own arrangements.

154 Co-regulatory models are varied and can include legislation that:

(a) delegates the power to industry to regulate and enforce codes;

(b) enforces undertakings to comply with a code;

(c) prescribes a code as a regulation, but the code only applies to those who subscribe to it (prescribed voluntary codes);

(d) does not require a code but has a reserve power to make a code mandatory;

(e) requires industry to have a code and, in its absence, government will impose a code or standard; and

(f) prescribes a code as a regulation to apply to all industry members (prescribed mandatory codes).

## Advantages of co-regulation

155 Effective co-regulation has a number of advantages:

(a) *Expertise*—Compared with government and regulators, industry is considered to have greater understanding and knowledge of the conduct of industry participants and the markets in which they operate. This should mean that industry is best placed to craft regulatory solutions and take appropriate monitoring and enforcement action.

(b) *Flexibility and timeliness*—Compared to government and regulators, industry is typically able to respond to emerging regulatory problems in a more flexible and timely manner.

(c) *Cost efficiency*—Co-regulatory models ensure that the cost of regulation falls more efficiently on the industry that generates the need for regulation.

## Limitations of co-regulation

156 The limitations of co-regulatory models include that:

(a) they may lack credibility and public confidence;

(b) they may lack effective enforceability;

(c) they can prove to be anti-competitive in nature by creating inefficient barriers to entry.

## Characteristics of a successful co-regulatory model

157 While government backing is an important feature of a co-regulatory approach, this model is still typically devolved to industry to ensure implementation, monitoring and enforcement is carried out.

158 It is important that industry has sufficient resources, cohesion and incentive to do this effectively.

## When is government regulation needed?

159 The *Best Practice Regulation Handbook* states that 'explicit government regulation', typically comprising primary and often subordinate legislation, should be considered where:

(a) the problem is high risk, or of high impact or significance (e.g. a major public health and safety issue);

(b) the community requires the certainty provided by legal sanctions;

(c) universal application is required (or at least where the coverage of an entire industry sector or more than one industry sector is judged as necessary); and

(d) there is a systemic compliance problem with a history of intractable disputes and repeated or flagrant breaches of fair trading principles, and no possibility of effective sanctions being applied.

# Key terms

| Term | Meaning in this document |
|---|---|
| ADI | Authorised deposit-taking institution |
| AFS licence | An Australian financial services licence under s913B of the Corporations Act that authorises a person who carries on a financial services business to provide financial services<br>Note: This is a definition contained in s761A of the Corporations Act. |
| AIS | An account information service under PSD2 |
| AISP | An account information services provider under PSD2 |
| API | Application Programming Interface |
| APP | Australian Privacy Principles |
| AS PSP | An account servicing payment service provider under PSD2 |
| ASIC | Australian Securities and Investments Commission |
| CCR | The comprehensive credit reporting regime in Australia, which makes it easier for lenders to assess a borrower applicant's credit history |
| Code | The ePayments Code, which regulates consumer electronic payments in Australia, including ATM, EFTPOS and credit card transactions, online payments, internet and mobile banking and BPAY |
| Corporations Act | *Corporations Act 2001*, including regulations made for the purposes of that Act |
| EBA | European Banking Authority |
| EDR scheme | External dispute resolution scheme |
| EU | European Union |
| FCA | Financial Conduct Authority (UK) |
| FSI report | The final report of the Financial System Inquiry, released on 7 December 2014 |
| GDPR | European General Data Protection Regulation |
| OAIC | Office of the Australian Information Commissioner |
| OIDC | OpenID Connect |
| PIS | A payment initiation service under PSD2 |
| PISP | A payment initiation service provider under PSD2 |

| Term | Meaning in this document |
|---|---|
| Privacy Act | *Privacy Act 1988* |
| PSD | The first Payment Services Directive, implemented through the Payments Services Regulations 2009 (UK). |
| PSD2 | The revised Payment Services Directive |
| PSPs | Participating service providers under PSD, including credit institutions, electronic money institutions, post office giro and payment institutions.<br>Note: 'Payment institutions' are providers of payment services unconnected to the taking of deposits or the issuing of electronic money |
| Review | The Australian Government's Review into Open Banking in Australia |
| s761A (for example) | A section of the Corporations Act (in this example numbered 761A), unless otherwise specified |
| UK | United Kingdom |