Review into Open Banking in Australia
Secretariat
The Treasury
Langton Crescent
PARKES ACT 2600

By email: data@treasury.gov.au

23 March 2018

Westpac Group Submission – Review into Open Banking: Final Report ('Review')

The Westpac Group (**Westpac**) thanks Treasury for the opportunity to participate in the Review process.

In addition, Westpac supports the submissions made to the Review by the Australian Bankers' Association (**ABA**) and Business Council of Australia (**BCA**).

Introduction

Westpac strongly supports the development of an enhanced and safe data-sharing regime in Australia. Data, when used safely, effectively and by trusted users, provides immense value to customers, industry, the government and society more broadly. Improvements in our collective use of data will ultimately help Australia's global competitiveness through a more innovative and productive economy.

To achieve this vision, industry and government must have a shared objective of increasing trust and confidence in the protection and sharing of data across the Australian economy. In addition, the establishment of appropriate consumer-centric privacy safeguards, identity and security credentials must be considered of equal value to competition and innovation policy drivers in a data sharing economy.

While a customer can be compensated for fraud losses, a customer cannot easily be compensated for a stolen identity or the impact of other breaches to their privacy, including personal safety. It is therefore essential that the move towards an Open Banking Regime occurs in a manner that protects customers' data and financial assets and mitigates the introduction of systemic risk into the Australian financial and payments system.

Research demonstrates that customers support innovation and competition, but not if there is the risk that their privacy or security is not maintained. This is not just a theoretical concern: EY research shows that recent data breaches have already materially impacted Australian customers' appetite for data-sharing[1].

The objectives of the Open Banking Regime announced in the 2017 Federal Budget ('the Budget') were to:

- provide customers with greater access to, and control over, their banking data; and

[1] EY Global Customer Banking Survey 2016 – January 2017: 60% worry about accounts getting hacked and worry about the amount of personal information government and private sector organisations hold about them. 91% feel uncomfortable with their transactions being searchable by anyone on the internet

- support competition in financial services leading to better services, more choice of providers and lower prices.

Westpac's previous submission to the Review recommended these should be complemented with the following objectives:

- Protect each individual's identity, data and finances;
- Increase customers' trust in the banking and financial system; and
- Retain incentives for banking and financial services organisations to invest in data capture, secure data storage, management and analytics (this includes the ability for businesses to exchange data on the basis of commercial terms).

The preservation of commercial incentives for organisations to collect and add value to data was one of the key factors considered by the Productivity Commission (PC) when assessing options for improving data availability and use[2].

Westpac therefore supports the guiding principles which underpin the Review, namely: "customers, choice, convenience and confidence".

Westpac notes this Review is specifically focussed on 'Open Banking' in line with the Budget announcement. However, Open Banking should be viewed as the first element of a broader economy-wide data-sharing regime. Indeed, if the objective is to put the power of customers' data in the customers' hands, this policy position should apply to customer data irrespective of particular sectors or industry segments.

Westpac is therefore pleased that the Government has announced the establishment of a comprehensive 'Consumer Data Right' in response to the Productivity Commission's *Data Availability and Use Inquiry*[3] ('PC Inquiry') and the Review's recommendations on principles of reciprocity and equivalence.

Support for Review recommendations

In line with Westpac's previous submission to the Review the following recommendations are supported:

- Flexibility – allowance for competing approaches to develop and a recognition that Open Banking should not be mandated as the only way that banking data may be shared and compliance with the Consumer Data Right to be established.
- Regulatory efficiency – Leveraging existing legislative and regulatory frameworks (including the *Competition and Consumer Act 2010* ('the Competition Act') and the *Privacy Act 1988* ('the Privacy Act')) to ensure efficiency in the set-up of the regulatory and governance framework.
- A strong and transparent central governance regime with a central regulator responsible for the establishment of rules and standards in consultation with industry, a robust accreditation process with clear criteria for accreditation, ongoing monitoring and enforcement and customer dispute resolution.
- The automatic accreditation of Authorised Deposit-taking Institutions (ADIs) based on existing privacy, data and security credentials and a tiered accreditation system for non-

[2] Productivity Commission *Data Availability and Use*, Draft Report, pg 295
[3] Productivity Commission *Data Availability and Use*, Final Report, March 2017

ADIs based on the risk profile of the data being shared and the likelihood and consequences of harm.

- Provision for intermediaries such as middleware providers in the accreditation framework.
- Continued protection of personal information under Open Banking through the Privacy Act, a requirement that all accredited parties comply with the Privacy Act and, in principle, certain modifications of the Australian Privacy Principles.
- Level Playing Field – embodied in the principle of reciprocity between data recipients and data holders and the principle of 'equivalence' for data held by non-ADIs.
- The exclusion of enriched, aggregated and 'value added' data sets from the scope of Open Banking.
- The allocation of liability between participants, pursuant to a clear and comprehensive framework, under which participants are liable for their own conduct and not the conduct of other participants.
- The requirement for data sharing to be initiated by the customer and consent to be explicit, fully informed and able to be permitted or constrained according to the customer's instructions.
- Creating an access right for customers to empower them about how their data is used and a recognition of the need for customers to have a 'fair exchange of value' for consenting to a data sharing arrangement under the Regime.
- A comprehensive customer education process involving both industry and Government to ensure improved 'data literacy' and understanding of rights and responsibilities, risks and rewards associated with data sharing.
- Support for the development of an innovative and competitive Australian data industry.

Westpac's Alternative Recommendations

There are a number of recommendations in the Review that require careful consideration to ensure the identified policy objectives are achieved and important guiding principles are adopted.

Westpac's recommendations include:

- A phased approach to implementation commencing with consumer and small business deposit products and consumer credit card products available through online banking today.
- Commencement of a transition period once the Regime's rules and standards have been established.
- Carve-outs for large businesses, outcomes of identity verification assessments and data sets categorised as commercial-in-confidence, proprietary, sensitive or legally privileged.
- Supporting non-digitally active customers to access Open Banking through assisted activation of online banking.

- Amendments to the proposed liability framework, including who should be liable in particular circumstances.
- Minimum security requirements based on internationally recognised best practice and a publicly available address book of accredited parties.
- Accreditation requirements which include minimum capital and insurance requirements to ensure customers have recourse for losses under a consumer protection framework.
- Consideration should also be given to a last resort compensation scheme for less capitalised participants.
- Industry-led development of rules and standards (enforceable through the regulator).
- Development of Australian data transfer standards which permit the use of a redirect approach as opposed to a decoupled approach.
- Standard, plain-English wording for use-cases and a determinative list of use-cases to be provided to customers to ensure consent obligations can be appropriately understood and discharged.
- Consideration of a right to deletion/ right to be forgotten and a cost-recovery model.
- Westpac considers the existing privacy regime is appropriate and should be retained for the purposes of Open Banking.
- A single dispute resolution model to cover data-related disputes that are inherently broader than privacy and confidentiality.
- Establishment of a multi-disciplinary expert panel to support the regulator, proposed Australian Data Standards Body and dispute resolution mechanism.

These recommendations and other issues are discussed in further detail below.

Westpac Recommendation 1 – Implementation Timeframe

The Review has suggested that implementation should commence with the four major banks (Westpac, National Australia Bank, ANZ Banking Group and Commonwealth Bank of Australia) and recommends that a twelve month compliance period commence from the date of the Government's response to the Review.

One of the Review's key supporting arguments for this timeframe is a comparison between the requirements of the United Kingdom (UK) open banking regime and the proposed Australian Regime. The nine financial institutions mandated by the UK Competition and Markets Authority (CMA) Order on Open Banking ('the CMA9') were given eighteen months to comply with 'read' and 'write' functionality requirements. In contrast, the terms of reference of this Review were 'read only' and the Review therefore concluded that less time would be required for Australian ADIs to comply.

Westpac does not agree with the implementation timeframe recommendation in the Review.

First, while the Australian Open Banking Regime is 'read only' the scope of customers, products and channels impacted (including non-digital channels) by the Review's recommendations are significantly broader than the UK Regime.

For example, the UK Order applied to the transaction data of retail and small business current accounts accessible through online banking. Conversely, the Review recommends application to current and former customers, retail, small and large business customers, an expansive product list beyond current transaction accounts (including deposit and credit products) and a requirement for customers to access the Regime through non-digital channels. The implementation and risks associated with execution are therefore multiplicative. As it stands, the requirements would impact every business unit across Westpac including BT Financial Group, Consumer Bank, Business Bank and the Westpac Institutional Bank (WIB).

Second, even if a reduced scope was mandated, longer timeframe are required for the design, building and testing of significant technology, data and operational requirements. These are discussed further below.

1.1 Technology requirements

While the technological capabilities required to support Open Banking may be conceptually straight-forward, the design, build and testing of those capabilities are significantly complex. Under the current proposed scope, the required data sources are spread across a large number of existing technology applications that service Westpac's products, brands and channels. Many of the data sets proposed by the Review are not currently made available digitally to customers through online banking. Ensuring that our current and legacy systems can scale with the new demand for data access and sharing will be critically important to maintaining customer trust and confidence in the Regime.

The Regime will require the locations of mandated data sets to be identified and utilisation of new or enhanced technologies to source, ingest, integrate, prepare and securely transfer the data into the required format, standards and quality for external consumption. Data specific internal and external Application Programming Interfaces (APIs) will also need to be developed to enable access to this data from different existing systems and then provided to customers and data recipients via online banking.

The need to ensure appropriate quality and efficacy of privacy and security credentials cannot be underestimated due to the sensitivity of the data under the Regime and our commitments to protect our customers. This includes rigorous data governance standards around the creation of a centralised, readily accessible customer record of transactions, authorities and consents across channels, products, systems and brands within the Westpac Group.

Significant enhancements are required to ensure Westpac can comply with the requirements for a complete set of data capable of external release[4]. The design and build of an Open Banking compliant central customer record is a significant requirement to ensure that all customer-provided data can be extracted, integrated and delivered with confidence[5].

1.2 Customer and distribution channels

Significant changes to customer and distribution channels will also be required, including: user authentication, data recipient authentication, consent capture and subsequent data recipient

[4] The Review notes: "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… 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."

[5] Defined as "information provided directly by customers to their banking institutions". For example, 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.

authorisation. Each of these represents a significant technology change with separate design, testing and implementation work.

It is essential that there is adequate time for customer education and awareness raising. This is particularly important to ensure data participants can discharge their obligations with respect to informed and explicit customer consent.

1.3 Security

Strong privacy and security controls are fundamental to establishing, and maintain, customer trust and the success of the Open Banking Regime. Given the potentially large number of externally facing API connections into an accredited white list of data recipients, there needs to be adequate time to design and test the reliability and security of these new process and data transfer flows and cybersecurity credentials.

1.4 Operational requirements

Beyond technical compliance with the Regime there are significant operational requirements that need to be established or revised. These include support infrastructure, governance, ongoing monitoring, risk, compliance and audit frameworks and staff training. Design, build and testing of these requirements is essential to ensure rapid scaling as Open Banking evolves from the initial stages of establishment and customer adoption.

1.6 The need for reduced scope

The twelve month timeframe recommended by the Review (from the date of the Government's response to the Review) is therefore unfeasible for the suggested scope. Compliance timeframes should also recognise the substantial amount of regulatory reform programs the industry is currently implementing. There is a significant volume of regulatory reform in the data space occurring both internationally (e.g. the extra-territorial impact of GDPR) and domestically (e.g. comprehensive credit reporting (CCR). It is important to ensure that the intersection of these programs and requirements are considered as part of the Open Banking Regime and a holistic approach to policy reform is adopted.

If the scope was reduced to include products and data sets currently made available by the four major banks via online banking, compliance would be more achievable within 12 months from the finalisation of Rules and Standards. This includes, for example, transaction data relating to current transaction accounts and consumer credit cards. In addition, Westpac recommends that required data fields reflect the fields that are provided today to ensure timely implementation. We note, however, that there may be some variance in the specific data fields currently provided by ADIs as well as variations in data quality. Compliance deadlines should reflect that any uplift required to data fields and data standards which exceed current practices will require additional timeframes for implementation.

In addition, if the scope of the Regime includes data which is not currently available through online banking channels, a longer period will be required to prepare the data.

1.7 Dependency on Rules and Standards

It is also important to recognise that the industry's ability to meet implementation timeframes is contingent on the establishment of a central governance and regulatory regime and the development of appropriate data, transfer and security standards ('the Standards'). The Rules and Standards against which participants must build their systems and processes must be defined with the utmost clarity and precision and be finalised early enough to ensure implementation planning can be anchored to robust solution specifications.

The Review suggests that six months will be required for both the passing of legislation and the establishment of Rules and Standards which would leave ADIs with only six months to build and test solutions. Even with a reduced scope of customers, products and digital channel implementation only, Westpac's view is that six months is inadequate.

Given the large number of stakeholders to be engaged in the standard-setting process, it is possible that the establishment of the Rules and Standards would take more than six months to complete. A delay in the finalisation of the Rules and Standards would leave even less time to complete necessary solution architecture design and implementation.

1.8 A risk of systemic non-compliance

As the UK experience has demonstrated, the need to resolve significant outstanding issues in an Open Banking regime cannot be underestimated. This includes a risk assessment of the scope and sensitivity of the data and participants (including the potential harm that the data or participant could pose to the system), complexity of the processes involved (e.g. consent, authorisation and verification), privacy, security, liability, fraud and other impacts of data breaches on individuals. It is essential that an individual's identity, data and finances are protected and that trust in the financial system is retained.

These issues are not easily resolved even in jurisdictions that have been working on open-banking for several years. For example, the 13 January 2018 deadline set for UK Open Banking was initially achieved by three of the "CMA9" (noting two further banks have since been confirmed as compliant by the CMA). The CMA were forced to issue new directions for the non-compliant organisations and recognised, "*All of the CMA9 have different systems and ways of keeping information. While Open Banking will launch on the date specified by the CMA, some institutions will need more time in order to complete preparations for making Open Banking available.*"[6]

The Review notes that, "the ACCC should be empowered to adjust the Commencement Date if necessary", Westpac agrees that the ACCC should be empowered to provide an assistance compliance period. However, an appropriate timeframe should be set from the outset and this date should not be hardwired into the primary legislation.

Importantly, even if a regulator agreed not to take regulatory action in line with a legislative commencement date this would not prevent an individual from lodging a complaint with the regulator or approved external dispute resolution (EDR) scheme or taking action against an ADI for breaching the law. This leaves the ADI at significant risk of non-compliance and penalties. A regulator's agreement to not take action, despite a breach of the law, may also send a confusing message to consumers and undermine confidence in the Regime.

One of the key lessons from the UK is the need to work through these important and substantial issues before specific commitments or deadlines are set. This is to ensure timelines are realistic and achievable and do not put organisations in the difficult position of having to balance the risk of legal non-compliance with the risk of implementing an inappropriate or unsatisfactory design for customers.

[6] https://www.openbanking.org.uk/about-us/news/uks-open-banking-launch-13-january-2018/

Any 'mandated' timeframes should be avoided until relevant consultations are complete. Alternatively, given that the majority of the implementation activities by ADIs will be dictated by the Rules and Standards, the commencement date could be specified as a certain period after the Rules and Standards are finalised. Industry participants must agree to work with the ACCC and Government to ensure an achievable roadmap of compliance in line with stated policy objectives. Provision should also be made for the ACCC to amend timeframes and offer a period of assisted compliance.

Westpac Recommendation 2 – Implementation Scope

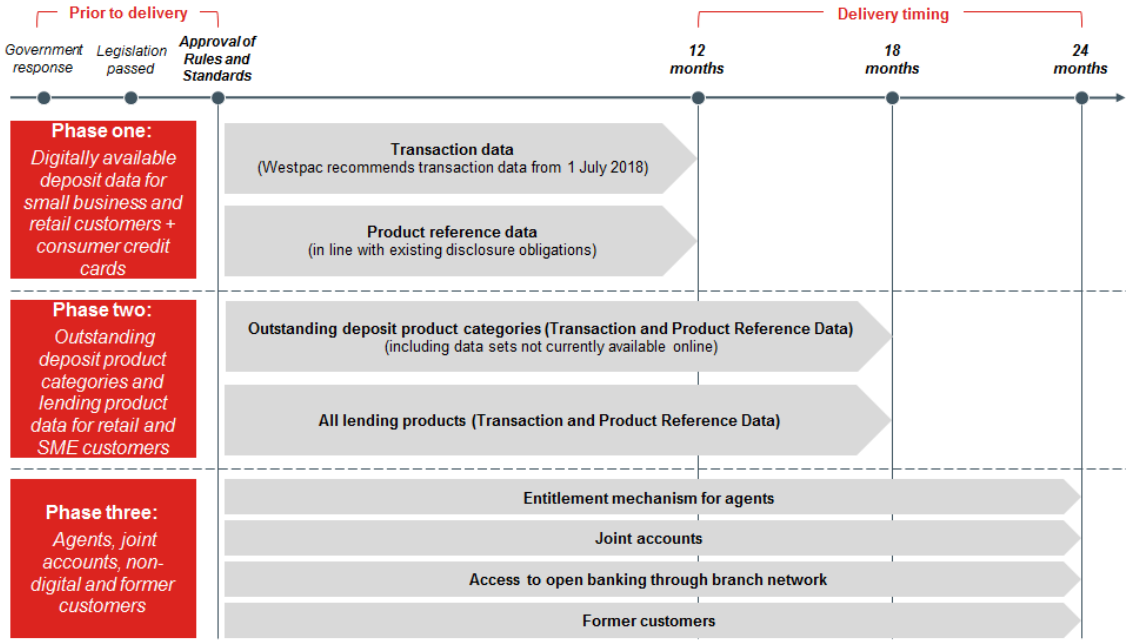
The Review recommends four data categories within scope of the Consumer Data Right in an Open Banking context:

1) Customer provided data;
2) Transaction data (which applies initially to transactions from 1 January 2017. However, we note, over time this requirement would apply to 7 years of historical data in line with existing record keeping requirements);
3) Outcome of an identity verification assessment; and
4) Product reference data (in line with existing disclosure obligations).

Transaction data and product reference data are identified in the Review as priority categories for implementation based on a list of designated deposit and credit products provided in Table 3.1 of the Review (see Appendix A).

One of the key trade-offs to be considered in the development of the Regime is time versus scope. As noted above, a 12 month compliance deadline for implementation is unfeasible. Westpac therefore recommends a phased approach to implementation (outlined in the diagram below). Westpac notes that a phased approach was adopted in the UK for retail and small business customers. Requirements for product reference data commenced in March 2017 and transaction data requirements were tested in January 2018 with implementation in March 2018 (approximately 18 months after the publication of the CMA report).

Westpac also notes that regulatory programs of a comparable scale and complexity are typically executed over three or more years.



It is important to note that Rules and Standards could be continuously iterated to support a phased approach to implementation. This principle of 'extensibility' is discussed further below under Westpac Recommendation five (5).

Westpac's proposed Phase One scope is captured in the table below and is in line with the PC's recommendation that the scope of data to be shared should be determined by industry[7].

Data Category	Purpose	Customer segment	Product	Channel	Timing
Transaction Data[1] *(Should apply to transaction data relating to transactions from 1 July 2018)*[2]	To allow customers to easily and safely share their transaction data (related to their use of a product or service), in a standardised, machine readable format, with third parties at the customer's request.	Current retail and small business customers	Deposit products (including savings and transaction accounts) and consumer credit cards	Digital (online banking)	12 month commitment on sharing this data, once relevant industry Rules and Standards are finalised.
Product Reference Data *(In line with existing disclosure obligations)*	To allow customers to easily compare products and offerings across the market through provision of data.				

[1] Where this data is currently available digitally through online banking; and required data fields are in line with what is provided to customers today. Enriched, transformed and value-added data fields would be excluded.
[2] This will ensure that transactions can be appropriately flagged on a prospective basis

[7] Productivity Commission, *Data Availability and Use*, Final Report, pg 20 "It is expected that industry sectors themselves would determine the scope of data to be transferred, subject to approval by the ACCC."

2.1 Product categories in Phase One

Westpac recommends that a number of criteria guide the inclusion of products in Phase One, including:

- **Current availability of transaction data digitally through online banking;**
- **Commonality of existing data fields across ADIs;**
- **Product penetration i.e. most commonly held by retail and small business customers;**
- **Product volume i.e. accounts for the greatest share of payment flows in the economy; and**
- **Ability for product transaction data to meet priority use-cases.**

Small business deposit products currently available through online banking across the Westpac Group would include: savings accounts, term deposits, transaction accounts, trust accounts. Other deposit products such as farm management deposits, foreign currency accounts and GST and tax accounts would be implemented in Phase Two as transaction data for these products is not currently available in a digital format to the customer through online banking. The only consumer deposit products in Table 3.1 not currently available through online banking are pensioner deeming accounts and retirement savings accounts.

Westpac and banking industry data confirms that transaction accounts and credit cards are the most commonly held, and utilised, products by retail and small business customers.

The inclusion of both types of data-sets ensures that use-cases related to income and expense verification for credit applications and approvals will be satisfied, facilitate ongoing compliance with responsible lending obligations under the *National Customer Credit Protection Act 2009,* as well as the provision of tailored offers, accounting integration and reconciliation services. This will also encourage innovation around personal financial management tools, including spend management and control.

It could also assist with account switching by providing a more comprehensive overview of recurring payments (credit cards) and direct debits on transaction accounts. However, Westpac notes there are outstanding issues to be resolved in the payments industry more broadly, with respect to the flagging and identification of recurring payments and direct debits[8].

It is important to note that customer and third party use-cases are likely to be enhanced through the introduction of Comprehensive Credit Reporting (CCR) and the New Payments Platform (NPP).

The significant amount of work required to standardise data field content, data quality and format to ensure data is in a common, machine readable form should not be underestimated. As noted above, Westpac's ability to comply with the scope recommended in Phase One will be dependent on the amount and nature of the standardised data fields required to be shared under the Data Standards. If the mandated list of data fields is comprehensive, a longer

[8] Due to Australian banks' limited ability to properly identify recurring payments from the data available through the Cards Scheme, substantive changes to the Cards Scheme will need to be negotiated to allow that data to be more accurately collected and made available to customers about their recurring payment transactions. The ABA is establishing a working group with ABA member representatives to scope the engagement plan with the Cards Scheme stakeholders regarding those negotiations. This is in line with the recommendation of the Khoury Review of the Australian Banking Association (ABA) Code of Banking Practice (2017).

implementation timeframe may be required to ensure compliance. For example, if credit cards were to be included in Phase One the required data fields should be limited to transaction date, transaction amount, and transaction description presented as term text including details such as merchant name. This would be in line with the data fields provided by ADIs today.

In addition, Westpac recommends that transaction descriptions, as a key data text element, should be standardised across the industry to aid consumer and data recipient understanding of transaction details and the usability of transaction data in the emerging Australian data industry.

2.2 Customer segments in Phase One Scope

The Review and previous Government inquiries have identified existing customer pain points within the retail and small business segments that could be successfully addressed through an Open Banking Regime. The same pain points and requirements have not been identified for large businesses, including the corporate and institutional customer segment (discussed further in section 2.5.1). Westpac therefore recommends that Phase One commence with retail and small business customers and that 'large businesses' are carved out from the scope of the Open Banking Regime.

The Review supports the inclusion of 'large businesses' on the basis that there is currently no agreed definition of small business and that "carving a set of customers out of scope could prove to be an additional cost, not a cost-saving" and "it might be harder to exclude large businesses than include them". Further consideration of this point is required. Westpac notes there are existing legislative, regulatory and industry definitions of small businesses that could be leveraged for this purpose.

For example, while the Privacy Act currently protects individuals, not non-individuals, it sets the threshold for regulated entities as $3 million turnover. In addition, the Australian Banking Association's recently revised *Banking Code of Practice* contains a definition of the small business[9].

As noted in the BCA Submission, *"Businesses are experienced in distinguishing between large and small businesses for regulatory purposes (for example, in relation to unfair contract terms, collective bargaining by small businesses or representation by the Financial Ombudsman Service)."*

Westpac supports a standard 'small business' definition being determined for the purposes of a Consumer Data Right being established across the economy.

[9] A business is a "small business" if at the time it obtains the banking service all the following apply to it: a) had an annual turnover of less than $10 million in the previous financial year; and b) It has fewer than 20 full-time equivalent employees (or it manufactures goods, it has fewer than 100 full-time equivalent employees)' and c) it has less than $3 million total debt to all credit providers – including: i) any undrawn amounts under existing loans; ii) any loan being applied for; and iii) the debt of all its related entities that are businesses.

3. Proposed subsequent phases

Phase	Inclusion	Timing
Phase 2	(a) Outstanding deposit product categories for retail and small business customers (including data sets not currently available through online	18 month transition period from the finalisation of the Rules and Standards
	(b) All lending product categories for retail and small business customers	
Phase 3	(a) Entitlement mechanism for agents (including lawyers and accountants for small business)	24 month transition period from the finalisation of the Rules and Standards
	(b) Entitlement mechanism for retail consumers and joint accounts (retail and small business customers)	
	(c) Access to Open Banking available through branch network as anon-digital channel (via access to online banking)	
	(d) Former customers	

2.4 Phase Three scope

a) Agents

The Review recommends that a customer should be able to authorise an agent to request data to be shared on behalf of that customer and the agent should be able to access that data once authorised. Or alternatively, a customer could ask the data holder to issue an agent with a credential that allows the agent to authorise sharing of information with the third party without the agent requiring access to the data directly.

Managing consents for data sharing via the use of agents raises complexity in relation to identification, verification, authorisation and validity of the underlying consent itself. Westpac will need to build a consent management process across four online banking platforms and ensure different 'entitlement' structures can be captured for each small business customer.

Westpac therefore recommends agents are within the scope of Phase Three to ensure these workflows, processes and requisite uplift in security can be implemented appropriately and to limit any delay in the delivery of Phase Two (outstanding product segments for retail and small business customers).

In addition, where the customer has directed an agent to request sharing on their behalf the customer will need to provide authority for the agent to represent the customer. This will need to include authority to give informed consent on the customer's behalf and authority to accept these risks on behalf of the customer (as the holder will be unable to discharge informed consent responsibilities directly with the customer). 'Agency' also needs to be considered under the proposed intermediary model. The ability for data recipients to pass on data received from the original data holder to another party (as an intermediary) will need to be carefully considered. Westpac considers that the ability to pass on data received from another participant creates reduced accountability.

b) Joint accounts

Recommendation 4.7 of the Review suggests that "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."

In line with the above comments, joint accounts also raise complexity in the management of consent. Given the suggested liability framework, Westpac considers it preferable for consent to be provided by both account holders in advance of the data sharing taking place rather than consent being addressed retrospectively (through termination or withdrawal). The existing approach for the provision of eStatements for joint accounts (whereby both parties have to indicate consent) provides a potential model for implementation.

Such a model would mitigate the risk that there is a lack of consensus between account holders for the purpose of a data sharing arrangement, particularly given that the applicable data applies to the provision of information by, and transaction activity of, both parties.

Inclusion of joint accounts in the Regime will require data holders to:

- undertake a large consumer engagement program (to recapture consent for the purpose of data sharing arrangements);
- customer education (to ensure the risks associated with data sharing are appropriately understood and accepted and the consent is both informed and explicit); and
- an online workflow authorisation capability (this is costly and requires time for design, build and implementation).

Finally, it may be appropriate for the industry, Government and regulators to assess whether any exemptions from the 'joint consent' model are appropriate on the basis of defined use cases. For example, whether a distinction should be drawn between a data sharing arrangement supporting a financial services verification for the purpose of applying for joint debt (where both parties should provide consent) or individual debt (where either party can consent).

c) **Non-digitally active customers**

Recommendation 5.9 states that data sharing should be authorised by customers who do not use online banking, through service channels which are ordinarily provided by the data holder[10].

The benefits and policy rationale for including non-digitally active customers in the scope of the Regime are not clear in the Review nor is there evidence that the benefits for such customers

[10] Recommendation 5.9

will outweigh the costs and the significant operational complexity associated with implementation.

For example, there is no clear evidence that non-digitally active bank customers would engage with other third parties in a digital manner (e.g. utilisation of personal financial management tools). This suggests that the customer segment utilising Open Banking is likely to align to digitally active bank customers. In contrast, non-digital bank customers currently relying on physical correspondence are likely to interact with third parties on this basis.

Nevertheless, Westpac agrees that the rights and features of an Open Banking Regime should be made available to customers that do not currently use online banking. 86% of eligible Westpac customers (based on the product sets currently available on online banking) are registered for online banking.

An 'in branch' support model

Westpac recommends that non-digitally active customers access Open Banking through an in-branch staff-assisted process (as a designated non-digital channel)[11]. This would enable non-digitally active customers to share their data through a once-off, temporary or ongoing activation of online banking. However, there are still a number of administrative and operational challenges that will need to be addressed under this model. For example, whether consent would need to be captured through a physical form in the presence of a banker.

Westpac previously submitted to the Review that online banking is the optimal safe data-sharing solution to capture consent, identify and authenticate customers and third parties and facilitate the data transfer to third parties. This proposed 'in branch support' model will allow the existing online banking capability developed in Phase One to be leveraged. Capturing customer consent and the authorisation and verification of an accredited data recipient through online banking will also ensure:

- the ADI has full visibility of customer authorisations;
- the data holder can interact with the customer in a timely manner (including for the purposes of fraud detection); and
- the customer, the data holder and the data recipient are able to view a single and reliable digital source of truth and

Other non-digital channels

ADIs should not be required to facilitate data sharing through any other non-digital channels, including a telephone banking environment, given the significant risks associated with fraud, privacy breaches and identity takeover. Even if a customer commenced a data transfer process over the phone a customer would still be required to attend a branch to complete the data transfer request.

[11] Or another face-to-face channel designated by an ADI.

It is also unclear how ADIs would implement the other requirements of the Regime in a non-digital environment including, persistent authorisation, reauthorisation of consent after a designated period, customer directed revocation of consent, a central consent dashboard for active consents, explicit and informed consent (managed through single-screen notification in digital channels) and a record of data sharing usage history (as required by Recommendations 5.6[12] and 5.11).

For example, if a bank was required to mail out a physical notice of new consents and authorisations to a customer, thismay reduce the customer's ability to identify fraudulent or incorrect data transfer requests in a timely manner. This is in contrast to a customer's ability to authorise a transfer in a branch environment where standard branch identification and verification processes can be utilised and a record of the transfer can be provided directly to the customer. Any requirements for the physical mail-out of documents would also be a significant additional cost to data holders and should be considered as part of a cost recovery model (discussed in Westpac Recommendation 11 below).

Westpac commits to undertake a customer awareness campaign and support our customers to activate online banking to share data under the Open Banking Regime in a branch environment (as a designated non-digital channel). This will expedite Westpac's ability to fully implement Open Banking.

d) **Former customers**

The Review recommends that data holders should be obliged to share a former customer's provided data (where this is held in a digital form) directly with the customer and transaction data with a third party at the customer's request.

There are a number of outstanding issues that would need to be addressed to enable 'former customers' to be within the scope of Open Banking. For example:

- How a 'former customer' is to be defined and whether there is a maximum threshold (e.g. access to data from a terminated relationship for a maximum period of 12 months from the date of termination). Such an obligation would need to apply prospectively to ensure systems can be established to facilitate access to the historical data of closed accounts.
- It is unclear whether an ADI would be required to provide online banking or an alternative portal and interface to enable former customers to have read access to mandated data sets within closed accounts. Currently access to online banking ceases once a customer relationship is extinguished and online access is not provided to closed accounts. A cost recovery model for this type of service would need to be considered given that access to banking services (including online banking) are provided as part of a current bank-customer relationship.

[12] 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 (i.e. should not be in perpetuity), 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.

2.5 Recommended out of scope segments

2.5.1 Large businesses

Westpac notes the inclusion of large businesses is an expansion of the scope originally recommended by the PC. In addition, the BCA (as an association representing large businesses) has recommended that 'large businesses' are carved out from the scope of the Open Banking Regime.

A clear policy rationale has not been identified which would justify the inclusion of large businesses within the scope of the Open Banking Regime. To the contrary, there are multiple evidence points which demonstrate existing competition within the corporate and institutional banking market. For example, a significant proportion of customers currently maintain multi-bank relationships (including with domestic and foreign banks), banking relationships are often subject to complex (re)tender programs with customers and the sophisticated nature of the customer compared to the retail and small business market.

In line with the BCA and ABA submissions, Westpac supports a recommendation to carve out large businesses for the following reasons:

- Nature of the authority - Westpac does not agree that the authority for data sharing should equate to an existing payments authority. There are different considerations and risks associated with authorising payments versus authorising data sharing and specifying how a data recipient may use that data. This is a significant issue given the commerciality (and potential market sensitivity) of the data involved with an organisation's financial position.

  In practice a de-facto reliance on 'payment authorisations' could mean the entire accounts department of a large institutional customer would have authority to direct the transaction history of that organisation to be shared with a third party for a period of up to seven years.

- Consent - There are different considerations for, and there is a higher degree of complexity with, a business consent regime. The requirement to have "explicit and informed consent" is far more difficult to discharge with a business as opposed to an individual. For example, it is unclear ADIs could ensure that individuals within a customer's business are educated about the risks associated with data transfers and the consent obligation is appropriately discharged.

- Identification and verification of appropriately authorised individuals - Approved or authorised persons within a large business are likely to change from time to time.

  It is unclear how appropriately authorised individuals within each organisation would be communicated to data holders and data recipients (for example, whether a 'white list' of authorised representatives within large businesses would be publicly available). Even if a white list was made available, an ADI and data recipient would need to find a way to identify and verify those individuals even where there is no existing relationship or identity documentation held by the ADI on those individuals. This is particularly important as the Review's liability framework proposes an ADI would be liable to an individual customer for transferring their data on the basis of a request from another individual, who was subsequently shown to not be appropriately authorised.

- 'Customer of the customer' - Inclusion of transaction data for businesses could potentially include confidential information of third parties. For example, payroll data for organisations contains salary details of individuals, which could be exposed to the data recipient. In that circumstance, the data recipient has effected secondary collection of confidential information of an individual which may be deemed to be personal information under the Privacy Act. This is also an important consideration for small businesses which would need to be considered in the context of the consent and liability frameworks. For example, a customer would need to confirm they have the necessary rights to allow the data to be shared and should be liable to the bank for any associated liability if the bank has followed a valid direction to transfer the data and the customer is subsequently determined not to have the necessary rights. In addition, the bank should not be responsible for the actions of a data recipient.

- System complexity - It is unclear how the other requirements of the Regime (e.g. consent control dashboard) would be implemented for large business customers given that large businesses do not utilise 'online banking' in the same way retail customers do.

- Cost – Westpac therefore does not agree with the Review's conclusion that the incremental cost of including large businesses in the scheme would be insignificant nor that exclusion may prove more costly than inclusion.

  By contrast, we observe that the technology used to deliver banking services to large companies, particularly the online banking interface, is completely different to the environment for retail and small business customers. Currently, there are no shared technology components between Westpac's retail online banking system (Westpac Live) and our large corporate online banking system (Westpac Corporate Online). Consequently, including large corporates in the scheme approximately doubles the implementation cost at this layer.

2.5.2 Outcome of identity verification assessment

Westpac does not consider that the inclusion of the data category on 'identity verification assessment'[13] aligns to the Review's commitments to supporting competition. Westpac has previously submitted that the policy objective of competition is intrinsically linked to the concept of a 'level playing field'. It is important that competitive neutrality and a level playing field are maintained. Established organisations should not be expected to subsidise, or absorb business costs on behalf of, other data participants in data-sharing initiatives.

Westpac is committed to supporting the development and enablement of portable digital identity in Australia. This will lead to significant improvements in customer experience, shared and enhanced Know Your Customer (KYC) processes and payments fraud. There is considerable work being undertaken by both the Government and industry on digital identity (including directly by banks and through industry associations such as the ABA and Australian Payments Council). This work is in addition to the current consultation by AUSTRAC and the Attorney-General's Department on changes to anti-money laundering legislation.

It would therefore be premature to include identity verification within the scope of Open Banking given a workable model and associated costing has not yet been implemented.

[13] Recommendation 3.4 – *Identity verification assessment* - "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."

Costs associated with identity verification assessment outcome

The Review suggests that the charging model for this data category should be based on the liability borne by the original verifying entity[14]. Westpac is of the view that liability should be considered separately to the economic model of pricing for identity verification assessments. An original verifying entity should be permitted to recover its costs even if the risk to the verifier does not increase as a result of other parties' reliance on it.

Westpac also does not agree with the Review's suggestion that "the cost recovery model (defined as marginal cost of the activity) should be virtually nothing per individual transaction" given that the original verifying entity would have "incurred the costs of performing the verification regardless of whether or not subsequently instructed to share it". As noted above, the principles of competition should ensure that organisations are not subsidising other participants in a data sharing economy, particularly those entities that cannot provide an equivalent identity verification service. Westpac should therefore not be expected to absorb the significant costs associated with identity verification assessment and then provide this outcome to another data recipient for free.

Westpac notes there is an existing process for pricing approval through the ACCC that could be leveraged for the purposes of approving reasonable cost recovery activities.

Provision of identity related documents

Westpac notes the Review's recommendation that information supporting an identity verification assessment should only be shared directly with a customer and not a data recipient (Recommendation 3.1). Importantly, the Review acknowledges that supporting documentation provided by an individual as part of identity verification is one of the most common methods of identity theft.

Risks related to fraud and unauthorised access to the customer's accounts are significantly increased by the provision of certain identifying information to a third party, including the customer's date of birth or copies of a passport/ drivers licence information. Westpac has been taking active steps to remove personal and identifying information from online banking due to the increased use of screen-scraping and the ability for fraudulent parties to access this personal information to take over a customer's identity.

Westpac recommends data holders should not be required to share information supporting an identity verification assessment directly with the customer for these same reasons. If data holders were required to supply personal information about a customer (e.g. identify information) inside a digital channel such as an online banking system this would become another vehicle for identity theft (and increase online banking as an attractive target for malicious actors). An additional uplift in security credentials would be required at a significant cost to the organisation.

[14] Recommendation 3.11 – *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.

Westpac recommends that the outcome of an identity verification assessment is removed from the scope of Open Banking even if the anti-money laundering laws are amended to allow data recipients to rely on that outcome. In addition, a carve-out should apply to any data that materially increases the risk of customer identity theft and data holders should not be required to share information supporting an identity verification assessment with the customer directly or data recipients. If an outcome of identity verification assessment remains in scope, original verifying entities should be permitted to recover reasonable costs (as authorised by the ACCC).

Westpac Recommendation 3 – Exemptions from in-scope data categories

As noted above, a key consideration for the PC was the balance between encouraging innovation and competition and retention of commercial incentives for organisations to collect and add value to data. This has been acknowledged in the Review through the inclusion of a carve-out for transformed, value-added[15] and aggregated data[16]. Therefore, Westpac does not agree that the inclusion of aggregated data sets in the scope of Open Banking should be revisited at a later point in time.

The specific definition of 'value-added customer data' and 'aggregated data sets' will be particularly important and Westpac looks forward to the Standards consultation process to ensure these important carve-outs are captured.

In addition, Westpac recommends there is specific exclusion of:

1. *Commercial-in-confidence/proprietary information* (including data used for internal business decisions and the outputs of models and other calculations, such as credit, risk or other rating models).These constitute core commercial and competitive assets of participating organisations and organisations make considerable investments in order to develop tailored and competitive services;
2. *Other sensitive information*. There are certain types of sensitive information that would not be appropriate to provide to consumers (or their nominated third parties) even where this is requested or consented to by the consumer. For example, data required to be collected under regulatory requirements relating to financial crimes and suspicious transaction reporting which by law must not be shared with any third party or a customer's online banking or other passwords due to the risk of fraud / unauthorised access to the customer's accounts; and
3. *Legally privileged information*.

3.1 National interest datasets

The three data categories above are not suitable for release even on an aggregated or de-identified basis or where there may be a public benefit to do so. The Review notes that the PC

[15] The Review suggests this includes data that results from effort by a data holder to gain insights about a customer. For example: 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.

[16] The Review suggests this data set is created when banks use multiple customers' data to produce de-identified, collective or averaged data across customer groups or subsets. For example: average account balances by postcode or income quintile, or average size of small business overdrafts by industry segment.

encouraged the publication of more data by public sector agencies in the national interest as 'National Interest Datasets'.

Consistent with Westpac's response to the PC, Westpac does not support a recommendation to compel ADIs to share commercial-in-confidence/ proprietary information in the national interest beyond what is otherwise required by law. Such data should continue to be shared with third parties on a voluntary basis, in a secure and controlled manner and on commercial terms through the use of private data marketplaces and bilateral arrangements. This will support the Review's objectives to support and enhance both competition and confidence.

3.2 Cleansed data

The Review defines value-added customer data as "data that results from material enhancement by the application of insights, analysis or transformation by the data holder"[17]. Westpac considers that cleansed transaction data (e.g. clear description of transaction text, correction of misclassified merchant name and merchant category code fields) would comply with this definition if the Data Standards are below the existing standards used by ADIs today with respect to cleansed and uncleansed data. ADIs should only be required to share data to a consistent standard as all other ADIs and participants. Higher quality data should be considered out-of-scope for Open Banking in order to retain market forces of competition with respect to the investment that is made to enhance and improve data assets.

Proposed carve-outs for transformed, value-add and aggregated data should be retained and specific provision should be made for commercial-in-confidence/ proprietary, sensitive and privileged information and data.

Westpac Recommendation 4 – Liability Framework

1. Allocation of liability

Westpac agrees with the Review's recommended allocation of liability in Recommendation 4.9[18] which draws on existing legal frameworks. Westpac's previous submission to the Review noted data holders should be in no worse a position than they are today in relation to liability risks. We agree that the receiving party must take sole responsibility and assume all liability for any use (or misuse) of data once transferred from the ADI, including the obligation to keep the data secure. In addition, there are also circumstances in which a receiving party may be liable during the transfer process as outlined further below.

Westpac agrees that an ADI should not be liable to a customer for a data breach suffered by a data recipient which impacts the customer's data after it has been transferred (even if the bank continues to hold the same dataset on its own systems). This principle is reflected in Case Study Six of Table 4.2[19] in the report, "The accredited data recipient has received the data securely by the bank. However the data recipient suffers a data breach impacting a number of customers."

[17] Recommendation 3.3 (and subject to Recommendation 3.4)

[18] 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.

[19] Pages 67-68

However, Westpac disagrees with the proposed unequivocal allocation of liability to an ADI in Case Study Five[20], where "a malicious actor manages to intercept the customer's data during the transmission between the bank and an accredited data recipient".

There are also certain circumstances in which an ADI, as data holder, should not be liable for malicious interceptions given that the data transfer process is not wholly within an ADI's control nor should an ADI be liable where the malicious act arises from deficient security safeguards on the part of the data recipient (i.e. the interception arose during the data transfer as a result of an act or omission on the part of the data recipient). In these circumstances the data recipient should be liable.

4.2 Identification of breaches

The need to instill a culture of transparency and the regulator's ability to identify data and security breaches are significant issues that need to be addressed as part of the next phase of consultation to ensure that consumer and participant confidence in the Regime are established and maintained.

Westpac notes that establishing the root cause of a data breach (to ensure responsibility is correctly allocated in accordance with the principles in the liability framework) may be complex due to the:

- Method of breach – some examples of data breaches may be identified months or years after the breach event first arose;
- existence of multiple copies of data held by different entities;
- number of parties potentially involved in a data breach; and
- requirement for co-operation and sharing of information in relation to the breach.

Identifying the root cause of a breach (in order to determine responsibility in accordance with the framework) is likely to be a time and resource intensive exercise. A mandatory data breach reporting Regime is unlikely to suffice on its own for this purpose.

The Standards should require a common level of breach prevention and detection capabilities by all participants to ensure a level of objectivity and consistency in the management of data and data breaches to support actual or suspected data breach incidents. A framework is also required to enable participants to raise suspicions of a data breach to the regulator on reasonable grounds.

4.3 Address book of accredited parties

The current liability framework suggests that if a data holder transfers a data set to a data recipient above their accreditation, the data holder will be liable. A data holder is therefore required to determine the accreditation level of a requesting data recipient. This reinforces the importance of Recommendation 2.9[21] and the regulator's responsibility to maintain an up-to-date listing of accredited participants on an address book as well as ongoing monitoring to reflect any necessary changes to a participant's level of accreditation.

The address book must be system-readable, continuously available in real time (within the required performance rate of the transaction), and include details of how a data recipient should be authenticated (e.g. using a cryptographic means, like public key). Westpac recommends that a listing on the address book becomes a de-facto safe harbour.

---

[20] Page 67

[21] 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.

4.4 Accreditation standards

The liability case studies in the Review reinforce the importance of accreditation standards and the development of a whitelist of compliant participants. The concept of a whitelist is embedded in the European Union's PSD2 directive and consequently the UK Open Banking Regime.

Westpac strongly recommends that in addition to compliance with data, transfer and security standards, accreditation requirements should also include minimum capital and insurance requirements which may include professional indemnity insurance or the expansion of the recently established insurance market for data liability or cyber-insurance. These minimum requirements are important to ensure data participants have the financial standing for any customer losses that may arise from operating the Open Banking Regime and provide customers with appropriate recourse in the event of a data breach or data misuse.

4.5 Customer recourse for losses

Consideration of the need for customer recourse for losses as part of a strong consumer protection framework is essential. For example, the Australian Competition and Customer Commission's (ACCC) Scamwatch reported $84 million worth of customer losses relating to scams in 2016. It is expected scams would increase in an open data environment.

In 2017, Westpac compensated customers $42 million for fraud losses. We expect identity related loss events to rise under a Regime where personal financial information is shared directly with data recipients digitally due to:

- an increased ability for malicious third parties to impersonate customers and fraudulently transact on their behalf; and
- likely security breaches of individual transaction data held by an authorised third party.

We have estimated additional future annual fraud losses under an enhanced data-sharing Regime as being between $90 million and $250 million for Westpac customers alone. In addition to increased actual losses for the bank, the extrapolation of these losses across the industry suggests an inherent systemic risk across the banking system and industry. These fraud risks are heightened in a real-time payments environment enabled through the New Payments Platform. This shift to real-time payments increases the likelihood that the money has gone by the time a fraud pattern has been detected[22].

It is currently unclear whether third party data participants would have the capital to adequately compensate customers where they are liable for the data breach. A possible lack of recourse to compensation and the rise of uncompensated losses would lead to broader costs to the Australian economy. For these reasons, Westpac recommends that a last resort compensation scheme is mandatory for participants that have capital levels below a minimum threshold.

Nevertheless, it is important to note that even with appropriate controls and regulation in place, Open Banking is expected to lead to an increase in losses which must be borne by individual participants, the banking system and Australian economy more broadly.

[22] For example, this occurred in the United Kingdom when the 'Faster Payments' initiative was introduced in 2007. During 2007 and 2008 online banking fraud losses more than doubled the period prior to the introduction of real-time payments (from £22.6 million in 2007 to £52.5 million in 2008 and £59.7 million in 2009). Source: https://www.pymnts.com/news/security-and-risk/2017/faster-payments-fraud-cybersecurity-biocatch/

Further consultation on the practical application of the proposed liability framework is required, including the intersection with the accreditation framework and mandated Security Standards. In addition, the consumer protection framework must provide clear customer recourse for losses. Consideration should be given to a last resort compensation scheme for less capitalised participants.

Westpac Recommendation 5 - Development of Rules and Standards

Westpac considers that a holistic model for Open Banking would be best executed through a clear division of roles, where:

- the *Government* plays a central role in establishing the legislative framework for safe data-sharing and the Consumer Data Right across the economy ;
- *the regulator* assumes primary responsibility for administering the accreditation regime, approving industry standards and protocols, monitoring and enforcing industry compliance with those standards i.e. the appointed regulator should play dual approval and enforcement roles; and
- the *industry* comprises the banking sector, fintechs and advisory panels of technical experts, community representatives and other related parties. Industry should play a leading role in the design and development of common standards (data, transfer and security standards) and protocols for safe data-sharing.

Drawing on the lessons learnt from the UK experience, Westpac considers Australia can establish itself as a 'smart leader' in the development of Rules and Standards by adhering to the following guiding principles:

- Industry-led - A mechanism for industry-led design thinking for the development of the Rules (solution requirements) and Standards (technical solution).

  This approach enables the adoption of a top-down regulatory framework for safeguarding and managing economy-wide data-sharing, with a bottom-up, industry-led approach for establishing the technical standards and protocols for sharing of banking related data in a safe and secure manner. This is consistent with the PC's Final Report which noted the regulatory framework for open data will need to create a broader consumer right that balances economy-wide standardisation and industry-level adaptation[23]. Westpac notes industry codes of conduct already play an important role in regulating financial products and services in Australia[24].

- Expertise – Ongoing mechanism to leverage of the expertise of the banking industry in the key areas of privacy, security and fraud management, provide input into the minimum requirements of accreditation standards and assist the regulator make determinations on participants. For example, a central expert panel could support the regulator and independent data specialist as Chair of the proposed Australian Data Standards Body.

[23] In its Final Report, the PC recommended that a standards-setting process be established under new legislation to allow the ACCC to register an industry-agreed scope of consumer data and agreed standards for transfer and data security, and that industry should start immediately to define data-sharing rules and industry-level data specification agreements. (Productivity Commission, *Data Availability and Use* – Final Report, pg 337)

[24] For example, ASIC's Regulatory Guide (RG) 183 outlines ASIC's approach to approving industry-created standards and enabling industry members to 'opt-in' to models of conduct and disclosure to improve consumer confidence.

The importance of capability and expertise has been reinforced by the UK experience.

- Sustainability - The sustainability of the framework over the long term which can flexibly respond to technological advancements and emerging risks. The Rules and Standards should be technology neutral in line with the Review's recommendation. Overly prescriptive standards should be avoided to ensure innovation is not stifled in the Australian market.
- Extensibility (in line with Recommendation 5.3[25]) – A focus on the feasible development of base standards to implement the first phase of Open Banking (this includes a consideration of the time required for the definition and implementation of the relevant Standards).

  A base standard will ensure interoperability and efficiency but will not prevent the evolution of standards to support additional phases (including additional customer, product and data scope as well as additional data fields).

  Data product scope and transfer mechanisms should be incorporated by reference into the Standards to ensure they can flexibly respond to changes in user requirements and technological innovation (including data transfer mechanisms and processes for the management of consent, authorisation and verification processes).

  In addition, participants should not be prohibited from extending beyond the core mandated standards in line with the 'competition' and 'choice' pillars of the Review.
- Consistency - Setting industry-wide and specific data standards, including standardised wording/ language in term text fields, data quality and data standardisation of format and content descriptions.

The Review proposed that the Rules will be set by the ACCC as the proposed regulator and Standards will be developed by the Standards Development Body in consultation with industry (and the two streams will work in parallel). Given the Rules will set the requirements and the Standards will provide the technical solution for implementation it is essential that the process to develop the Rules and Standards is not disjointed or in conflict.

Westpac recommends that the industry is given six months to establish draft Standards and these are used by the regulator to finalise the Rules and Standards. The Data Standards Body should provide the secretariat function for this process. If the industry does not establish the standards within this reasonable timeframe, the regulator can then impose Rules and Standards in consultation with industry.

Westpac Recommendation 6 – Data transfer standards

6.1 The UK Approach

As noted above, Westpac considers there is a significant opportunity for Australia to take a globally leading approach to safe data-sharing within banking and financial services. Rather

[25] Recommendation 5.3 - *Extensibility* – The Data Standards Body should start with the core requirements, but ensure extensibility for future functionality.

than simply being a 'smart follower' of other jurisdictions, including the UK, Australia should establish itself as a 'smart leader'.

Recommendation 5.2 of the Review does not follow this principle. Rather it suggests that the UK Open Banking technical specification should be the starting point for the Data Transfer Standards.

The Review's recommendation appears to be based on an assumption that Australia would be starting with a 'blank page' for the development of these standards. However, there are existing data transfer frameworks in the Australian market that could be leveraged (including frameworks that Australian ADIs currently have in place). Use of these existing Australian frameworks also aligns to the principle that standards should be 'fit for purpose' for the domestic jurisdiction.

Australia has a significantly different operating environment from the UK (which is currently grappling with the intersection between Open Banking, Revised Payment Service Directive (PSD2) and General Data Protection Regulation (GDPR)) and different policy drivers for the establishment of Open Banking (including an identified lack of competition in the retail overdraft market). Therefore, Australian standards should not simply transpose these UK and European standards, noting that many of these regimes already have an extra-territorial impact which includes Australia and/or Australians.

Westpac is actively participating in the ABA's technical architect and API expert working group. This working group is devising a framework for common Australian API standards by drawing on the lessons learnt from the UK technical standards and international best practice.

6.2 Redirect versus a decoupled approach

The Review recommends that while the UK's redirect-based authorisation and authentication workflow should be used as a starting point for the data transfer model, consideration should also be given to the merits of a decoupled approach provided it minimises customer friction[26].

The Review also concluded that multi-factor authentication[27] would be sufficient to protect customers in a redirect model. Westpac does not support this conclusion, nor the use of a redirect model to establish the Open Banking Regime.

Westpac had previously submitted that a 'pull' model, in which a third party website redirects to a banking authorisation layer to complete customer verification would be less secure than the data transfer relationship being initiated within online banking (as this starts the authorisation less request in a less trusted environment and exposes customers to increased phishing risk). However, we recognise the Review's conclusion that a mechanism solely based on a 'push model' would create friction between the third party and customer.

Westpac recommends that the next phase of consultation prioritise a solution design based on a decoupled model in line with a safe-data sharing approach to Open Banking.

[26] Recommendation 5.4 – *Customer-friendly authentication and authorisation*

[27] 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.

3. Concerns with a redirect approach

A redirect model would result in the data-sharing arrangement being initiated from the third party website and the provision of a form for the customer to enter their online banking credentials to complete the authorisation process (without the customer first navigating to a separate browser to enter the URL of their bank). This would make it difficult for a customer to distinguish between a bank's online banking website, and a 'phishing attack'.

In a phishing attack, a criminal creates a website that looks like a trusted institution, for example a bank or a government department, and induces customers to supply their username and password. Once surrendered, the criminal then either attempts to transact as the user at the legitimate site, or sells those passwords on to another criminal for that purpose.

The serious nature of this threat cannot be underestimated. In 2017, Westpac responded to 2118 unique phishing sites which attempted to convince customers to disclose their banking passwords, and 225 unique banking-specific malware that attempted to compromise one of our brands[28]. Each of these involved material effort on the part of the attacker, in expectation of a return.

There is existing evidence to suggest that malicious attackers are aware of the security gaps in redirect models. For example, mimicking of Mastercard 3DSecure and Verified by Visa. This reinforces that multi-factor authentication is not enough to mitigate the inherent security risks in a redirect approach as the customer has provided their username and password directly to a malicious actor and multi-factor authentication is therefore never invoked.

In addition, Westpac is committed to increasing customer education about the need to protect themselves from fraud, identity theft and malicious actors. A redirect model undermines the key messages of the consumer education campaigns which have been run by ADIs and other organisations over the last fifteen years including to remind customers:

- never to provide their online banking credentials to anyone except their bank;
- never to click on bank URLs contained in emails, websites and applications;
- to only enter their password after typing the URL of their bank directly into a separate browser address bar. This is in line with our

A redirect model may also mean that protections otherwise available under the ePayments Code may not be available to the customer depending upon how the redirect workflow is structured. For example, the bank may not compensate for fraud on the customer's account resulting from the use of the customer's password or other access information or credentials. A redirect model could therefore limit the effective uptake of the Regime (as a result of customer mistrust) and is at odds with the Review's commitment to enhancing confidence.

6.4 The benefits of a decoupled approach

There are several benefits associated with a decoupled approach over a redirect approach:

- A decoupled solution aligns with customers' stated desire to start from a position of trust[29].

[28] Westpac also analysed another ~900 viruses which may have affected customers, including password-copying viruses and ransomware.

[29] Major bank research demonstrates only 7% of Australians feel comfortable giving their bank permission to share personal and financial information with an internet start-up not certified by their bank.

A decoupled approach would still enable a data sharing arrangement to be commenced from a third party website but would encourage the customer to go separately and directly to their existing online banking site to complete the authorisation of the relationship, and to revise/revoke existing relationships with third parties. This could include the use of tokens between the third party website/ application and the ADI to reduce friction.

- A decoupled approach utilising online banking gives customers strong protection by leveraging existing security credentials.

  Completing the third party relationship and data-sharing transaction within online banking puts the sensitive operation within the high-side, trusted environment where additional protections can be implemented such as second factor authentication A key element of defending against cybersecurity threats is the controls inside our online banking channel; in particular, those which can differentiate between a user and a computer using their password. This is particularly important given customers are often unaware of the risks they take with their personal data when they provide permission to third parties, despite information being available on this topic.

- This mechanism aligns with a key principle of the UK open banking regime, namely that banks are responsible for authenticating and verifying the identity of the customer and third party recipient.

In addition, this solution would have the added benefit of the customer's online banking platform becoming the 'hub' or single interface for a range of data-sharing consents with third parties. In a scenario where the customer wishes to switch providers, the account could be switched with relevant consents in place, rather than changing those consents with multiple providers (currently a key barrier to switching). Westpac therefore considers that the ADI should manage consents relating to ADI-held data in the first instance[30]. However, alternative and future models of consent management should not be restricted, including self-sovereign models of consent.

Nevertheless, it is important to recognise that a decoupled approach does not completely mitigate the cybersecurity risks identified above.

Westpac Recommendation 7 - Security standards

Westpac endorses Recommendation 4.8 of the Review i.e. In order to be accredited to participate in Open Banking, all parties must comply with designated security standards set by the Data Standards Body.

7.1 Increased risks

Westpac previously submitted that a 'safe data-sharing' approach in banking must take into account the following systemic risks:

- First, a significant data breach under the Regume could result in large scale identity theft and a loss of trust in, and the integrity of, the financial and payments system; and

- Second, the frequency and sophistication of cybersecurity attacks continues to increase.

[30] The ability for data recipients to pass on data to another party (as an intermediary) will need to be carefully considered. For example, the ability to pass on data received from another participant creates reduced accountability.

As noted above, the move towards sharing of personal financial information with third parties will increase the risk of data interception, identity theft (social engineering or impersonation of customers) and fraudulent transactions. This is particularly the case where third parties have lower security standards and/or less robust privacy safeguards than the banking industry, making the relevant data more vulnerable to unauthorised access, hacking and misuse.

This has serious consequences for the safety of customer funds, their personal identity (e.g. stolen identity) and the physical safety of our customers (e.g. in the instance of a domestic violence scenario where transaction data may be used by a potential perpetrator to draw inferences or collect information about a victim's location). This reinforces the benefit of a whitelist approach under Recommendation 2.9 to ensure customers can distinguish between an appropriately accredited data recipient and un-licensed players.

In the banking and financial services context, customers expect that information maintained by a bank will be kept confidential and be held to the most rigorous data security standards. The design of Open Banking must recognise and reflect the position of trust customers hold their financial institutions to in safe-guarding their finances, data and identity[31]. Customers should not be expected to accept lower data security and privacy standards in the financial services industry under an Open Banking Regime than they currently enjoy today.

Westpac is continuously monitoring our environment for vulnerability to cyberattacks and investing in both new cyber security controls and enhancements to prevent fraud as the attacks from malicious parties increase in volume and sophistication. A recent industry study suggested that one ransomware[32] gang alone netted US$325 million in payments from victims[33]. The Federal Government's Australian Cyber Security Centre saw a 300% increase in these kinds of ransomware attacks in 2015 over 2013[34]. The same report indicated that half of all respondents had experienced a cybersecurity incident in the preceding year.

The Australian Prudential Regulation Authority has recently released a new package of rules for the financial sector designed to increase the ability of financial institutions to mitigate cyber-attacks and to respond swiftly in the event of a breach. In part, these measures are necessary because of the value to an attack of the type of data that the banking and financial services industry hold.

7.2 Security requirements for 'data about money'

The Review draws a distinction between a bank dealing *with* money versus *data about money*. This is used to suggest that the prudential and security obligations imposed on banks to protect customer funds and the integrity of the payments system may not be fit for purpose for an Open Banking Regime dealing with data *about* money.

However, the strength of accreditation standards, including minimum security requirements, should not be conceded because data is only 'about' money. Both customer provided and transaction data provide the means for a malicious actor to facilitate transactions (e.g. via

---

[31] 68% of Australians most trust banks to safeguard their financial information, compared to 3% for internet start-ups. An online survey commissioned by CBA on behalf of the major banks through an independent research panel conducted between 16th February 2017 and 1st March 2017. Sample: nationally representative sample of 2536 Australians (Major Bank research). In the Australian Community Attitudes to Privacy Survey 2017 – people trust banks and Government the most when it comes to privacy risk (59% for banking/ finance and 58% for Government) - https://www.oaic.gov.au/resources/engage-with-us/community-attitudes/acaps-2017/acaps-infographic.pdf

[32] Malware which encrypts user's data and then offers to return it after payment

[33] Source: https://cyberthreatalliance.org/pr/pr-102915.html

[34] Source: https://www.acsc.gov.au/publications/ACSC_CERT_Cyber_Security_Survey_2015.pdf

identity theft). Indeed, the new mandatory data breach reporting obligations reflect a customer expectation that their data will be protected in the same way as their financial assets. Less stringent standards could create systemic risks of data breaches, undermining the important security role banks play in our economy which is often taken for granted. Stringent accreditation and security standards are therefore required.

Westpac notes the Regime is not intended to create barriers to entry. 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. For example, the appropriate control and management of any 'honeypot' of personally identifiable data.

7.3 Monitoring of compliance

Westpac agrees with the Review's recommendation that "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." However, the enforcement and monitoring elements of the regulatory framework need to go beyond self-assurance by the participants to ensure compliance. Mandated, annual, external audits should form part of the regulatory framework.

Nevertheless, it should be recognised that any increased third party access to data and moving data from bank-grade security to third parties with less rigorous security systems, controls and processes (including in relation to secure data storage) will increase the risks to consumers and the likelihood of systemic risks in the financial system. This includes the increased risk of data interception, identity theft (social engineering or impersonation of customers) and fraudulent transactions.

Westpac Recommendation 8 - The use of supplemental standards

The Review suggests that "supplemental, non-binding, standards to develop (provided they do not interfere with interoperability) will encourage competitive standards-setting and innovation." However, it is not clear what these "supplemental standards" would include and the method for adoption.

Westpac previously submitted that bilateral participation agreements could be used to deal with particular issues between participants (data holders and recipients). We acknowledge the Report's conclusion that relying on a process of bilateral negotiations would be 'unworkable' to facilitate the broader Consumer Data Right in a data sharing economy. However, Westpac submits that supplemental standards could permit the use of bilateral agreements to cover particular issues of importance that are not currently dealt with in the Review's proposed regulatory framework. For example, negotiable terms such as pricing/commercials and permitted use rights and restrictions which can be documented in a pro forma schedule to the agreement.

As noted above, the use of commercial arrangements will help retain incentives for private sector organisations to invest in data capture, secure data storage and analytics and continue to ensure innovation, including the ability for businesses to exchange data on the basis of commercial terms. These bilateral participation agreements should be enforceable through contract law outside of the overarching regulatory framework and associated liability framework.

Westpac Recommendation 9 – Consent management process

As noted above, Westpac strongly supports the principle of a customer-centric approach to safe data-sharing in banking, and open data across the economy more broadly. This includes the principles of:

- Opt-in and customer directed data sharing;
- Informed and explicit consent to ensure the customer knows exactly what they are consenting to, the scope of data to be shared and timeframes for transfer of data e.g. one-off or continuous and risks associated with data-sharing;
- Provision of an mechanism to turn consents on and off and to view current consents (including central consent dashboard); and
- Intended use-case identification (to ensure monitoring of use-case compliance by the regulator e.g. data shared for the purpose of a credit decision (not for ongoing offers or re-use of data by other third parties).

Westpac recognises the Review's conclusion that "customers are best placed to determine value of services". However, Westpac recommends that the Data Standards include a taxonomy for use-cases (standard set of use case categories and wording) to ensure consistency across data participants and enhanced consumer education.

Clear, concise and effective consent needs to be provided for all use-cases, not just those which the Review identifies as "particularly sensitive" such as marketing, on-selling, sharing of data or sending of data overseas. Rather than providing a 'summary of possible use cases' to which a customer's data could be put, the single screen notification should provide a determinative list of intended use-cases. While competition will naturally drive innovation in use-cases, the Open Banking Regime must define service offerings and a mechanism to ensure the evolution of use-cases over time are captured by the Standards.

Even where a customer has nominally consented to the data transfer, they may not fully appreciate the type or amount of data that may be disclosed about them, how that data will be used by the third party (e.g. whether the third party might sell the data to other parties) or which types of data attract a higher risk of fraud. For example, according to the OAIC currently only 29% of Australians read privacy policies[35].

Westpac recommendation 10 – Right to deletion

The Review recommends against a right to deletion being included in the Open Banking Regime[36] (in contrast to the PC's recommendation). Instead the Review suggests that if a data recipient "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." However, without a right to deletion or a right to be forgotten (or conversely an obligation to expunge the data), the regulator's ability to control the use of data (once a consent has expired or has been revoked) becomes extremely difficult.

[35] OAIC Community Attitudes Report (2017), pg 31. Source: https://www.oaic.gov.au/resources/engage-with-us/community-attitudes/acaps-2017/acaps-2017-report.pdf

[36] 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.

Westpac recommends that a right to deletion is considered within the context of specific use cases and subject to any overarching retention period required by applicable law. For example, if a customer authorises the sharing of data to a data recipient for the purpose of performing income and expense verification for a credit application, extending the scope of use beyond that purpose or continuing to use the data once that verification has been completed does not align with the individual consent. Similarly, data specifically provided under a time-bound consent should not be usable beyond that consent. However, a further discussion is required to assess whether a data recipient which no longer has rights to access and use the data should reasonably be expected to delete or expunge the data.

If consideration of a right to delete is determined to be outside the scope of the Regime, it should be acknowledged within the liability framework that any 'restriction' on this right will need to be carved out where it conflicts with other applicable (including cross-jurisdictional) privacy laws, i.e. GDPR. For example, it is unclear how a restriction on the right to delete under Australian Open Banking will stand up against the express 'right to be forgotten' under the EU GDPR (which Australian banks would be required to comply with if caught by the GDPR's extra-territorial application).

Westpac recommendation 11 – Cost recovery and the right to charge

Westpac has always maintained that customers should not be charged for the sharing of customer provided or transaction data within the scope of the Open Banking Regime in line with Recommendation 3.11[37].

However, Westpac considers a further discussion is required to determine whether a cost recovery or charge model should apply between participants in the Regime. An Open Banking Regime must recognise the economic value of data and retain commercial incentives to invest in data. In addition, Westpac disagrees with the Review's conclusions:

- that the costs associated with the establishment and operation of Open Banking (including transition and data transfer) would be small or negative when compared to the costs of data transfer under bilateral agreements or paper based requests;
- that "transition costs should be kept to a minimum if transfer mechanism is simple and does not require adoption of particular, expensive technology"; and
- ongoing costs would be low.

Further detail on some of the costs associated with the Regime is provided in Appendix B.

Westpac suggests there are two categories of cost recovery by a data holder that should be considered:

1) **Use of data by a participant for a customer-use case (in line with informed and explicit consent) versus ongoing use of the data by a data recipient or use for another purpose**

For example, once customer consent is withdrawn a data participant may not be permitted to use the data for a particular customer use case (e.g. financial services verification for the purpose of a credit application), however this would not prevent the data recipient from continuing to use their data for their own internal purposes (e.g. marketing segmentation) or commercialising the data as part of a de-identified and aggregated data set.

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

Westpac recommends that if a broader use is intended by the data recipient, this should be made transparent to the individual at the outset as part of the informed and explicit consent process. This could involve a distinction between use-case categories such as 'primary specified use', 'secondary use' and 'unrestricted use' in addition to the specific use cases being specified and consented to by the customer through a determinative list.

If a customer does not provide consent for a broader purpose, a data recipient should source this data through data marketplaces or commercial bilateral arrangements where broad use rights can be reasonably negotiated between entities.

2) Cost recovery associated with data and transfer costs (including API infrastructure, data sourcing, preparation and cleansing)

The PC recognised there may be costs to business associated with their adherence to a Consumer Data Right and economy-wide open data[38]. In recognition of this, the PC recommended that data holders (including private sector organisations and government) would be able to charge data recipients for costs reasonably incurred in transferring consumer data (including access/ sourcing and data preparation). A tiered model based on "effort" was considered to be appropriate[39].

As a starting point, a data holder could charge the recipient a reasonable service fee for each instance of a data recipient's access to the data holder's systems to receive data in line with a customer's consent.

This model would preserve organisations' incentives to invest in the implementation and maintenance of APIs through which a third party is able to access a customer's data. In addition, it may facilitate the participation of other organisations in economy-wide open data who may currently face barriers to establishing and maintaining the infrastructure required to comply with Open Banking. A cost recovery mechanism would also be in line with the UK Open Banking access charging model.

Westpac agrees with the PC recommendation that the ACCC[40] could be responsible for the review and approval of a schedule of cost recovery fees to ensure they reflect reasonable costs and the onus would be on data holders to explain these costs.

There could also be consideration of a cost recovery model above certain thresholds; for example, in line with a Declared Service Arrangement under Part 11C of the Competition Act. Criteria to determine an appropriate threshold may include:

- Frequency of access (API calls and data requests); and
- Data currency (i.e. updated and refreshed data feeds).

Regarding frequency of access (API calls and data requests), Westpac supports Recommendation 5.10 i.e. that the Data Standards Body should determine how to limit the

[38] Productivity Commission, *Data Availability and Use* – Final Report, pg 20

[39] Productivity Commission, *Data Availability and Use* – Final Report, pg 20: *"We fully expect that there may be a tiered approach to such charges, namely that some digital data that is of high quality, readily available, and clearly identifiable with a particular individual (such as transactions data), should be made available at low or no cost and at relatively short notice. Data stored on different (yet still digital) systems, or that is of lesser quality may require additional effort to provide in a usable format and therefore could attract a higher charge and take longer."*

[40] Productivity Commission, *Data Availability and Use* – Final Report, pg 21.

number of data requests that can be made by data recipients. This is in line with the Productivity's Recommendation[41].

Data currency and an assessment of whether data transfer requests need to be provided in near real time is an issue to be addressed under the Standards. Data currency is a key component of the technical and operational requirements and will require significant uplift to foundational architecture and user interfaces.

Finally, the Open Banking Regime should not restrict the ability for data holders to enter into bilateral or multilateral commercial data sharing and exchange arrangements.

Westpac Recommendation 12 – Principle of Reciprocity

Westpac strongly supports Recommendation 3.9[42] relating to reciprocal obligations in open banking and the principle that 'equivalent transaction data' should be shared by data participants. This includes the requirement that eligible entities need to participate as both data holders and data recipients. Non-ADIs should not solely be receivers of data with ADIs as only transmitters of data. As the Review notes, " 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 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."[43]

This is particularly important given the Consumer Data Right is intended to be economy-wide and the objective of establishing a robust and innovative data industry in Australia.

Westpac recommends that the Government urgently commence a consultation process on the principles of reciprocity and equivalence across industry segments. This consultation process should cover how the principle of reciprocity and equivalence will practically be applied, including within and between designated sectors as well as between accredited participants more broadly . This will require a discussion of guiding principles and specific criteria to determine data scope. A comprehensive and transparent consultation process will mitigate any concerns related to the principle of reciprocity being used to "unduly extend the scope of the system be stealth"[44].

Westpac Recommendation 13 - The Privacy Act

Westpac supports the recommendation that all data recipients (regardless of annual turnover) be subject to the Privacy Act. However, Westpac considers that some of the other proposed modifications to the Privacy Act may need to be considered further.

A key concern is that the proposed modifications may have broader implications for the way data is managed by regulated entities beyond the requirements of the Regime due to the intersection of data received under an open banking data transfer and data received or

[41] Productivity Commission, *Data Availability and Use* – Draft Report, pg 234: the Commission does accept that a fee determined by the data holder (with the fee model open to scrutiny by the ACCC) may be charged for each request.
[42] 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.
[43] Pages 43-33
[44] Page 44

generated through other means. Effectively there would be two separate regimes for the way data is managed based on how a regulated entity receives the data i.e. received directly from a customer or received from another data holder through a customer-directed consent under the open banking regime. It is important to ensure that the Regime does not inadvertently impact on current business practices in relation to data sets which are compliant with the Privacy Act.

Westpac's concerns relate to:

1. the proposed changes to the consent requirements; and
2. the removal of "reasonableness" qualifiers under the Privacy Act.

13.1 The proposed changes to consent requirements

Westpac recommends that if a data recipient receives "unsolicited" information pursuant to an individual exercising their rights under the Consumer Data Right, then an exemption should apply to the requirements that would otherwise apply under Australian Privacy Principle (APP) 4. A further discussion is required as to whether the data recipient should be permitted to rely on the requirement of the data holder to confirm informed explicit consent prior to sending the data to the data recipient, or if the data recipient should also need to confirm that consent with the individual. Westpac notes that the latter approach would add significant cost to the process.

We also note that if there is an appropriate exemption or amendment to Australian Privacy Principle (APP) 3 to ensure that a data recipient is able to receive personal information from a data holder rather than directly from the individual (as recommended by the Review), no changes may be required to APP 4.

13.2 The removal of reasonableness qualifiers

The proposed removal of the "reasonableness" qualifiers represents a significant uplift that would be extremely difficult for ADIs to comply within certain circumstances. This includes the Review's proposal for:

- reasonable steps to notify individuals under APP 5;
- use of personal information for secondary purposes reasonably expected by the individual under APP 6; and
- proposed uplifts to the application of privacy requirements to banking data under APP 7 and APP 8.

As outlined above, the difficulty arises as 'open banking' data would likely, over time, be co-mingled with other data about the individual to enable more meaningful and enriched use of data for the customer's benefit. However, the adoption of different Privacy Act requirements regarding handling and use of that combined data creates a two tiered regime which will either introduce significant cost or curtail existing use of data and associated innovation.

Westpac considers the existing privacy regime is appropriate and should be retained for the purposes of Open Banking, including in respect of the use of data for secondary purposes and disclosure of data offshore (for example, outsourcing service providers who support our business systems, subject to responsibilities under the existing APP8).

The existing safeguards under the Privacy Act recognise the importance of protecting personal information in a way that is reasonable and pragmatic for organisations, In our view, the underlying objective and 'spirit' of the Privacy Act should be maintained to enable APP entities to 'take such steps as are reasonable in the circumstances' to protect personal information. If

elements of 'reasonableness' are removed, compliance with the Privacy Act will become much more difficult to achieve and unnecessarily impede reasonable and responsible business practices.

Westpac Recommendation 14 - Multi-regulator model

Westpac previously submitted that the OAIC should be the primary regulator of Open Banking, noting that the existing remit of the OAIC would need to be expanded to support such a model. However, the Review has recommended:

- the Consumer Data Right be enacted through amendments to the Competition Act (to facilitate the designation of sectors); and
- a multi-regulator approach under which the ACCC will be the primary regulator with responsibility for competition and consumer issues and the development of standards supported by the OAIC (with continued responsibility for privacy protection and confidentiality issues)[45].

Westpac agrees that a central regulator should assume primary responsibility for administering the accreditation regime, approving standards as well as accountability for ongoing enforcement and monitoring and the consumer protection framework. Westpac reinforces that privacy and security should not be subordinated to competition policy drivers. It is important that 'competition' and 'confidence' have equal weighting under the Regime and an explicit recognition by the government that the maintenance of customers' privacy and security are essential to instilling confidence.

Westpac considers that a 'data protection framework' is required before a 'data sharing framework' for individuals and non-individuals can be established. In line with this, consideration should be given as to whether a stand-alone regulator is best placed to assume responsibility for the Open Data regime.

This may assist the Government to deliver on its objective to deliver an economic-wide open data regime underpinned by the Consumer Data Right. Alternatively, a separate dispute resolution mechanism should be established for all data related complaints (discussed further below). This would address a key current challenge where the regulator both supervises and protects regulated entities, in addition to refereeing disputes and complaints from individuals. It would also mean there is a central service for individual and small business data rights rather than the existing regulators having to expand their remit beyond individual consumer rights (and some small business rights in certain circumstances).

If the ACCC becomes the primary regulator, Westpac recommends a formal and structured relationship between the ACCC and OAIC to ensure the OAIC can provide constructive input and preserve the interaction between the Competition and Privacy Acts.

In addition, regulator access to expertise will be absolutely essential. There are likely to be industry-specific issues arising in the implementation, oversight and enforcement of the Regime that extend beyond competition or privacy issues which will require specific industry input and

[45] Recommendation 2.2 – 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.

knowledge. This may include access to data, security, cybersecurity, privacy and technical expertise.

Westpac recommends the Government consider the establishment of an 'expert panel' that can be drawn upon by the bodies involved in the Open Banking Regime.

These bodies may also include the Administrative Appeals Tribunal (AAT) and external dispute resolution bodies (such as the Australian Financial Complaints Authority (AFCA)). These bodies will require specialist divisions to deliberate on data related issues if a stand-alone dispute resolution mechanism is not established (discussed further below).

Westpac Recommendation 15 - Complaints resolution

A clear consumer protection framework is an essential element of a strong and transparent open data governance regime. Westpac agrees that this should include both internal and external dispute resolution. Westpac's previous submission to the Review noted that customers will both expect, and require, a clear remediation path if their data is not used in accordance with prescribed purposes and they suffer identity theft or other fraudulent activity or loss of funds as a result of that unauthorised use.

The proposed dispute resolution and complaints resolution pathways in the Review do not support a clear remediation path for customers or regulated entities. They also appear to conflict with the Review's acknowledgment that a single consumer contact point should be established. For example, the Review suggests:

- The ACCC should be given powers to address complaints and give customers standing to seek remedy for breaches of their rights under the Regime[46];
- The OAIC should retain enforcement powers in relation to privacy breaches (for individuals and small businesses) and could also be given enforcement powers of confidentiality disputes for small businesses[47]. Although the Review notes that "some business customer's 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"; and
- The OAIC should report all Consumer Data Right complaints to the ACCC.

The Review also suggests that customers could access other existing EDR schemes, including the newly established AFCA.

As noted above, Westpac recommends a single model for dispute resolution related to the Open Banking Regime which will cover data-related disputes that are inherently broader than privacy and confidentiality. There is an inherent risk that a model of 'split' responsibility for consumer data right complaint handling (ACCC) and privacy-specific / confidentiality enforcement (OAIC) could create confusion and inconsistency across the regime.

[46] Recommendation 2.10
[47] Recommendation 4.4

Related issues

1) PC Draft Report into Competition in the Australian Financial System ('PC Draft Competition Report')

Westpac notes that the PC's Draft Competition Report has invited suggestions on issues related to Open Banking. For example, the Commission has sought feedback on how liability for unauthorised electronic transactions should be shared, including whether liability arrangements should be addressed in the ePayments Code or whether the new Open Banking Regime could be relied upon as a better alternative for secured, shared access.

While Westpac will be responding separately to the PC Draft Competition Report, Westpac submits that the Open Banking model will be a better way of managing the security issues associated with shared access to banking data. We also support the Review's conclusion that the Open Banking model is likely to render practices such as "screenscraping" redundant, by facilitating a more efficient data transfer mechanism.

This also reinforces the importance of the liability framework i.e. that participants in Open Banking should be responsible for their own conduct, but not the conduct of other participants.

2) Comprehensive Credit Reporting

Westpac's submission on Comprehensive Credit Reporting (CCR) has noted the overlap between CCR and Open Banking, specifically with regards to data standards controls and on-going monitoring of data standard compliance. Currently, it is planned that ASIC and OAIC regulate CCR and the ACCC and OAIC regulate Open Banking (with the Data Standards Body establishing the standards). Westpac recommends that the Government consider the benefits of the Data Standards Body having responsibility for the development of data standards across both CCR and Open Banking.

Next Steps

Westpac welcomes the opportunity for further consultation with the Government on our recommendations and the issues identified in this paper. Westpac is committed to assisting the Review, including through our dedicated team of internal experts and formalised industry and standard setting processes.

If you require any further information about this submission please contact Jade Clarke, Director of Data Development & Innovation on jadeclarke@westpac.com.au

Appendix A: Table 3.1 – Review's list of proposed banking products within scope

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	

Appendix B: Costs

Implementation of the Open Banking Regime will require a range of solutions to be deployed across technology, digital, data and operational support streams. These will either be new capabilities or a significant uplift to existing capabilities will be required. For example:

- Establishment of foundational capabilities in the API platform before evolving to a more mature platform to support public APIs accessible by third parties
- Support for a complex entitlements, consent and access management solution for multiple parties
- A platform to serve customer and partner data transfer requests in near real time and the development of other new user interfaces.
- A robust operating model supporting partners and end user customers (including the ongoing maintenance, service and support of APIs (i.e., monitoring of performance levels and API version control)
- A multi brand transaction data repository to align with industry standards, including refresh requirements (which may be real-time).

Overall costs based on a phased, multi-year approach are expected to be in excess of $200 million. This estimate relates to upfront costs and does not take into account the cost of continued investment to implement, monitor and maintain the infrastructure for the Open Banking regime (including for example, API services, accurate and secure consent management frameworks and security requirements).

These costs need to be taken into consideration in light of the already very substantial cost of changing regulation that the industry is currently absorbing.