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

5 October 2017

Westpac Group Submission – Review into Open Banking ('Review')

The Westpac Group (**Westpac**) thanks the Open Banking Review for the opportunity to participate in the Review.

In addition, Westpac supports the submissions made to the Review by the Australian Bankers' Association (ABA), Australian Payments Council and AusPayNet.

INTRODUCTION

Westpac strongly supports the development of an enhanced and safe data-sharing regime in Australia. Data, when used effectively, 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.

For these benefits to be realised, industry and Government must have a shared objective of increasing trust and confidence in the protection and sharing of data across the Australian economy. Westpac considers this requires a strong and transparent central governance regime to be established in consultation with industry (including both authorised deposit taking institutions (ADIs)[1] and fintechs), regulators, customers and the community. To ensure appropriate privacy and security standards are maintained, Westpac recommends the method for data-sharing is tailored to the risk profile of the data being shared and the Government introduce enforceable data-sharing governance standards through a regulated licensing regime for all data market participants.

In addition, ongoing customer education about their rights and responsibilities is crucial. It is essential that customers recognise the value of their personally identifiable data and have an opportunity to manage it with the same controls they currently use to manage their money. Actively raising public 'data literacy' will also be important given customers are often unaware of the risks they take when they share their personal data, despite available information and disclosures on this topic. Both industry and the Government have a role to play in this education process.

Westpac notes this Review is specifically focussed on 'open banking' in line with the Federal Government's Federal Budget announcement ('the Budget'). 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.

[1] Authorised under the *Banking Act 1959*

In this regard, Westpac supports the Productivity Commission (PC)'s recent recommendations[2], namely:

- an economy wide open data regime should be underpinned by a comprehensive 'access right' for customer data[3]; and
- the particular scope of customer data should be determined by an industry-led process and subsequently authorised through specific technical standards and data specification agreements.

Westpac considers there is a significant opportunity for Australia to take a global leading approach to safe data-sharing within banking and financial services. Rather than simply being a 'smart follower' of other jurisdictions, including the United Kingdom (UK), Australia should establish itself as a 'smart leader'. In this regard, Westpac's submission outlines key lessons learnt from the UK and makes recommendations for the design and implementation of an Australian open banking regime.

Westpac notes, the objectives of the open banking regime announced in the Budget are to:

- Provide customers with greater access to, and control over, their banking data; and
- Support competition in financial services leading to better services, more choice of providers and lower prices.

Westpac considers 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).

Indeed, the preservation of commercial incentives for organisations to collect and add value to data was one of the key factors considered by the PC when assessing options for improving data availability and use[4].

In other words, an open banking regime should support competition and innovation while protecting the identity, security and privacy of individual customers and not undermining investment in data. Westpac's recommendations take this balance of objectives into account accordingly, as reflected in the proposed term of 'safe data-sharing'.

Research demonstrates that customers support innovation and competition, but not at the risk of their privacy or security being maintained. This is not just a theoretical concern: EY research

[2] Productivity Commission's Final Report on Data Availability and Use (Publicly released: 8 May 2017)
[3] Relates to an individual customer's use of a product or service and exempts commercial-in-confidence / proprietary information. Commercial-in-confidence information includes data used for internal business decisions, such as credit, risk or other rating models. Commercial-in-confidence/ proprietary information 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.
[4] Page 295 of the Draft Report

shows that recent data breaches have already materially impacted Australian customers' appetite for data-sharing[5].

In the banking and financial services context, customers expect that information maintained by a bank will be kept confidential and 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[6].

Increasing 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) may present undesirable risks for the customer. This is particularly the case if a customer directs that information is to be shared with a third party that is not currently regulated under the *Privacy Act 1988*.

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 open banking occurs in a manner that protects customers' data and financial assets and mitigates against the introduction of systemic risk into the Australian financial and payments system.

A 'safe data-sharing' approach in banking must take into account the following systemic risks:

- First, a significant data breach under any new open data regime could result in large scale identity theft and a loss of trust in, and the integrity of, the financial and payments system.
- Second, the frequency and sophistication of cybersecurity attacks continues to increase, which highlights the potential dangers of exposing personally identifiable data through new public Authorised Programming Interfaces (APIs).
- Third, the risk of a dramatic increase in fraud and associated losses due to the combination of a non-secure data-sharing environment, combined with the new instant-payment capabilities to be delivered by the New Payments Platform (NPP).

Currently, if a Westpac customer's account is compromised by internet fraud, through no fault of the customer[7], Westpac repays the customer for these missing funds. This includes circumstances where Westpac is not at fault. In 2016, Westpac compensated customers $57 million for fraud losses.

A significant increase in fraud losses under an inappropriately designed open banking regime would not only lead to increased actual losses for the bank, but also poses a significant risk to customers due to the rise of uncompensated losses, thereby impacting the Australian economy more broadly. Even with appropriate controls and regulation in place, we expect open banking to lead to an increase in losses.

---

[5] 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

[6] 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

[7] For example, this excludes scams.

This reinforces the need for the establishment of a clear liability regime to ensure the bank is not responsible or liable for the data once it has been provided to a third party in accordance with a customer's instructions. In addition, customers will require comprehensive education and a clear framework on the circumstances in which compensation and remediation can be sought (e.g. where a third party has not acted in line with the customer's consent or has insufficient controls and safeguards in place for the protection of customer data and fraudulent activity or loss of funds occurs as a result).

Finally, any open banking regime should put the customer at the centre. The regime should be designed around clear customer use-cases and answer the question – what does the customer want to do tomorrow that they cannot do today?

LESSONS LEARNT FROM THE UK

It will be important to continue to monitor and apply key lessons from the UK open banking regime, including any weaknesses in cyber-security and identity protocols and the rise of shadow banking (including from foreign government-owned entities).

The UK has sensibly drawn a distinction between a limited subset of 'open data' which relates to standardised product reference data (for example, pricing and terms and conditions) (known as Phase One) and 'sensitive, personally identifiable financial information' in Phase Two.

To date, the UK Implementation Entity has focused on the implementation of Phase One 'open data'. Delivery of this solution via open APIs was required by the end of quarter one 2017, in line with the CMA's deadline. This enables customers to easily compare banking products, including through third party comparison websites, and delivers on the CMA's policy objectives of increasing competition in the UK retail banking market and facilitating greater switching through greater product transparency.

The second phase of the UK regime is the sharing of personally identifiable financial information directly with third parties. In contrast to sharing 'open data' this is more complex and raises more significant concerns about the scope and sensitivity of the data, complexity of the processes involved (e.g. consent, authorisation and verification), privacy, security, liability, fraud and other impacts of data breaches on individuals. These risks exponentially increase where there is both 'read' and 'write' functionality (i.e. an ability for a third party to transact on behalf of the customer's accounts) as required by the CMA.

As the UK experience has demonstrated, the need to resolve significant outstanding issues in an open banking regime cannot be underestimated. It is essential that an individual's identity, data and finances are protected and trust in the financial system is retained. Recent discussions with stakeholders in the UK indicate there are still key issues which remain unresolved.

For example, the liability of the disclosing party and data recipient to each other and to the subject individual have yet to be worked through and adopting a regime whereby liability resides with the banks (e.g. PSD2) is not an appropriate allocation of risk.

Initial learnings based on feedback from UK stakeholders include:

- Establishing customer pain points and requirements up-front, to ensure the regime aligns to customer use-cases and creates real value for customers.
- A mechanism for industry-led design thinking and solutions development (including in the key areas of privacy, security, fraud management and liability).

- Establishing principles up-front to guide the development of the regime.
- Setting industry-wide and specific data standards, including standardised wording/ language, data quality and data standardisation.
- Early thinking regarding liability, customer compensation and increased losses. For example, this may include the development of a new insurance market for data liability or cyber-insurance.
- Consistent application of standards and security controls to all forms of data-sharing mechanisms (e.g. the use of APIs, private data marketplaces, bilateral direct transfer) to ensure consistency of customer experience and a level playing-field.
- A principles-based and technology neutral approach in regulatory/ legislative mandates. Sector specific data requirements, including data scope and transfer mechanisms should be incorporated by reference to ensure data standards can flexibly respond to changes in user requirements and technological innovation.
- Clear roles and accountability for the customer, ADI and third party. For example, the UK has established a principle that banks will take responsibility for verification and authentication of customer and third party[8].

Additional detail on outstanding issues in the UK is provided in Appendix 1.

GUIDING PRINCIPLES FOR AN AUSTRALIAN OPEN DATA REGIME

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

- Customer-centric approach – Ensure customer needs are met by providing real value and addressing current pain-points in a safe manner.
- Regulatory efficiency - Leverage existing legislative and regulatory frameworks to ensure efficiency in the set-up of the regulatory and governance framework.
- Sustainability - The sustainability of the framework over the long term which can flexibly respond to technological advancements and emerging risks.
- Trust - Start the customer data-sharing experience "from a position of trust" to ensure customer trust and confidence is retained and increased customer uptake of open banking e.g. online banking environment. This will be particularly important in the first phases of the introduction of open banking, and open data more broadly, in Australia.
- Expertise - Leverage the expertise of the banking industry in the key areas of privacy, security and fraud management e.g. Banks should retain responsibility for authentication and verification of customers and third parties.
- Liability - The receiving party must take sole responsibility for using the data appropriately, in line with the customer's instructions and expectations, and keeping the data secure. The third party must therefore assume liability for any use (or misuse) of the data once it has been transferred from the ADI. In particular, data providers will seek to be in no worse a position than they are today in relation to these liability risks.

[8] This could include leveraging existing two factor identification). Bank discretion will be maintained on the attributes required for authentication process e.g. username and password.

- Fairness - Fair exchange of value for the customer providing data to a third party.
- Level playing field - It is important that competitive neutrality and a level playing field are maintained. Established organisations should not be expected to subsidise new market entrants in data-sharing initiatives.
- Principle of reciprocity - Any participants that wish to seek access to customer data must also be set up to provide that data when requested. Mechanisms to reciprocate access to comparable information (on comparable terms) between comparable organisations exchanging data are also essential.

WESTPAC'S RECOMMENDATIONS

Westpac's recommendations have been designed in line with the suggested guiding principles above.

1. A phased-approach to safe data-sharing in banking should be followed

Westpac recommends a two-phased approach with additional time to ensure the appropriate design of a more sophisticated data-sharing solution for data that carries a higher inherent risk:

- ***Phase One*** – a mechanism to allow customers to easily compare products and offerings across the market through the provision of:
    - Product reference data for key products (pricing, product eligibility criteria, terms and conditions); and
    - Service data (e.g. branch and ATM location data).

In line with the ABA submission, Westpac supports a 12 month commitment on sharing product reference data and service data once relevant industry standards are agreed. The significant amount of work required to standardise data fields and formats to ensure data is in a common, machine readable form should not be underestimated.

- ***Phase Two*** – a mechanism to allow customers to easily and safely share transaction data (transaction accounts and credit cards) with third parties at the customer's request (personally identifiable transaction data).

In line with the ABA submission, Westpac supports a 24 month commitment for the sharing of retail and small business customer's transaction data with third parties in a standardised, machine readable format, once an overarching governance and regulatory regime is established.

This aligns to the phased approach adopted by the UK and is designed to prioritise customers' increased access to data about themselves in a timely manner. A phased approach will also enable lessons from Phase One to guide Phase Two and the future direction of open banking in Australia, which may include the use of partner APIs[9] or other technologies, such as data marketplaces that enable third parties to develop and test algorithms and insights.

[9] Westpac's categorisation of APIs is available in Appendix 2. A key difference between a public (open) API and a partner API, is the ability to combine technology controls with bilateral contractual agreements between participants in a partner API arrangement. These bilateral contractual agreements stipulate obligations on both parties, in particular to ensure the third party participant provides adequate controls to protect the customer's data and to protect the credentials they use to access the API.

Phase Two itself could be commenced as an initial proof-of-concept with a smaller subset of participants to test the efficacy of relevant data standards and security protocols and the effectiveness of a customer informed consent regime before the wider scheme is operational.

2. **Implementation timelines should only be set once a mechanism and process for industry and customer consultation is established and initial consultations are complete.**

Westpac has indicated support for a 12 month timeframe associated with Phase One and 24 months for Phase Two. The industry's ability to meet these timeframes is contingent on the establishment of a central governance and regulatory regime and the development of appropriate data and technical standards. We therefore consider any 'mandated' timeframes should be avoided until relevant consultations are complete.

As noted above, issues associated with the sharing of personal financial information directly with third parties have not been fully resolved in jurisdictions that have been working on open-banking for several years. One of the key lessons learnt from the UK is the need to work through these important and substantial issues before specific commitments or deadlines are set, to ensure timelines are realistic and achievable and do not put organisations in the difficult position of having to balance a risk of legal non-compliance and a risk of implementing an inappropriate or unsatisfactory design for customers.

Members of the UK Implementation Entity have suggested that the January 2018 deadline set by the Competition and Markets Authority (CMA) for the sharing of personally identifiable transaction data will be extremely challenging.

Our recommended approach is summarised in the below table:

Phase	**Purpose of mechanism to be developed**	**Data type**	**Timing**
Phase One	To allow customers to easily compare products and offerings across the market through provision of data.	*Product reference data* for key products (eg pricing, product eligibility criteria, terms and conditions).	12 month commitment on sharing this data, once relevant industry standards are agreed.
		Service data (e.g. branch and ATM location data).	
Phase Two	To allow customers to easily and safely share their transaction data, in a standardised, machine readable format, with third parties at the customer's request.	*Personally identifiable transaction data* relating to retail and small business customers' transaction accounts and credit cards.	24 month commitment on sharing this data, once an overarching governance and regulatory regime is established.

3. The method for data-sharing should be tailored to the risk profile of the data being shared.

As we outlined in our submission to the PC[10], there are a number of different ways in which information can be shared between organisations and their customers (and with their nominated third parties). For example, the use of public or bilateral externally-facing APIs, direct transfer and private data marketplaces.

Our submission to the PC also noted that while the transfer of data from an organisation to a customer carries some risk, there are additional privacy, security and liability issues that need to be addressed before financial or other sensitive information about a customer is shared with third parties. Westpac believes that the method for data-sharing should therefore be tailored to the risk profile of the data being shared.

For example, a public API platform could be utilised for the sharing of Phase One product-reference data, however this is not the most secure method for the transfer of personally identifiable transaction data in Phase Two. Indeed, the ability to effectively secure public APIs continues to be one of the most difficult problems for cybersecurity experts, as documented in a number of well-publicised API attacks over recent years. Westpac, considers that mechanisms such as online-banking would provide a superior and safer solution to the use of APIs for the sharing of transaction data. This reinforces why any permissive legislation should remain technology-neutral and should instead be captured in specific data standards developed by industry.

For example, as detailed in the ABA submission, online-banking could be enhanced to enable a customer to 'push' their transaction and credit account transaction data to a whitelist of third parties through an informed consent process. This mechanism aligns with a key principle of the UK regime i.e. that banks are responsible for authenticating and verifying the customer and third party recipient. In addition, this solution aligns with customers' desire to start from a position of trust. 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.

Westpac strongly submits that initiating a third party relationship and data-sharing transaction from within the trusted environment of online banking gives customers strong protection by leveraging existing security credentials.

Instead, if a third party requires that the data-sharing transaction is initiated from the third party website:

- It is difficult for the customer to distinguish between a bank's online banking website, and a phishing attack which replicates a bank's website; or
- Alternatively, such authorisation requests to a bank website would be functionally indistinguishable from cybercrime attacks.

In both instances customers are exposed, likely limiting the effective uptake of the regime (as a result of customer mistrust).

As noted above, an online banking solution would have the added benefit of the customer's bank account 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

[10] Pages 11 -13; Westpac Group Initial Submission to the Productivity Commission

switched with relevant consents in place, rather than changing those consents with multiple providers (currently a key barrier to switching).

A method which utilises online banking encourages the customer to go directly to their existing online banking site to authorise a relationship, and to revise/revoke existing relationships with third parties. This puts the sensitive operation within the high-side, trusted environment where additional protections can be implemented such as second factor authentication. 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.

Westpac considers the industry proposal for the transfer of personally-identifiable data is superior to alternative solutions, including:

1. An alternative 'pull' model, in which a third party website redirects to a banking authorisation layer (e.g. OAuth) to complete customer verification (as this starts the authorisation less request in a less trusted environment and exposes customers to increased phishing risk); and
2. The use of public APIs, due to the demonstrable complexity of securing APIs against concerted cybersecurity attacks.

Westpac acknowledges future innovation may enable alternative platforms and solutions to be leveraged (including, for example, a centralised digital identity utility and data marketplace solutions[11] to allow third parties to develop customer insights without the need to transfer raw, personally identifiable transaction data. However, online banking provides an existing solution that can be leveraged for the initial phases of delivery of open banking in Australia if the Government decides to require the sharing of transaction data.

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.

Currently, one of the primary mechanisms for cybercrime is phishing. In this 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.

Last year, Westpac responded to 1358 unique phishing sites which attempted to convince customers to disclose their banking passwords, and 150 unique banking-specific viruses that attempted to compromise customers' accounts[12]. Each of these involved material effort on the part of the attacker, in expectation of a return.

Westpac notes that screen scraping is widely used throughout the banking and financial services industry both domestically and internationally. Westpac considers that the continued appropriateness of screen scraping in an environment of open banking and comprehensive

[11] For example, Westpac has invested in Data Bank and the data exchange platform Data Republic. One of the main capabilities of Data Republic is that it offers a 'privacy by design' data marketplace platform which enables secure data storage, exchange and analytics of de-identified customer attribute data (such as spending patterns). This enables Data Republic participants to develop powerful insights across broad sets of data with extremely robust controls that reliably mitigate the risk of re-identification. Resultant data products such as propensity models and trends can be used to optimise, innovate and compete with existing products and services.

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

credit reporting should be discussed as part of a broader industry consultation process. However, any screen scraping conducted while these broader discussions take place, needs to be undertaken in a transparent and controlled manner with built in safeguards.

Screen scraping approaches utilised today require the customer to give their online banking credentials (i.e. username and password) to a third party. This essentially means that the bank cannot tell when it is receiving instructions from the real customer, or alternatively when those instructions are from a third party. In such circumstances, the customer is much more likely to experience fraud (e.g. as a result of a data breach at the third party) resulting in financial loss for the customer (as banking agreements generally disclaim liability where passwords are deliberately shared). In doing so, there is an additional risk that the customer's terms and conditions with the relevant bank will be breached and the protections otherwise available under the ePayments Code may not be available to the customer. 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 code information.

The frequency and sophistication of cybersecurity attacks continues to increase, which highlights the potential dangers of exposing personally identifiable data through new public APIs.

If ADIs were required to publish sophisticated open APIs to transfer personally-identifiable data, our capacity to detect and protect customers' compromised accounts would be significantly limited, with a resulting increase in both fraud and identity theft.

Among security experts, building secure APIs is well-understood to be a difficult problem[13]. Attacking APIs is an emerging specialty for security testing teams as part of the development and use of APIs[14].

As noted above, there have been a number of well-publicised API attacks and application security failures over recent years, including the leak of API keys through Android App in 2017[15] and the successful breach of the IRS in the US where 350,000 taxpayers accounts "were successfully accessed by unauthorised individuals" and a further 610,000 taxpayers "were at heightened risk of future identity theft"[16].

Further detail related to the definition and costs of APIs is provided in Appendix 2.

As noted above, a phased approach leveraging public APIs in Phase One for the sharing of product reference and service data and a non-API approach for the sharing of personal transaction data in Phase Two can be used to test the effectiveness of the regulatory framework and data standards.

In addition, this will allow alternative technologies to be tested, such as partner APIs or data marketplaces, including for the creation of algorithms and data insights by third parties without the need for personally identifiable transaction data to leave a secure and controlled environment. This would mitigate the risks and costs associated with third parties implementing

[13] Source: https://storage.googleapis.com/google-code-archivedownloads/v2/code.google.com/owasptop10/OWASP Top 10 - 2013.pdf

[14] Example: http://blog.smartbear.com/readyapi/api-security-testing-how-to-hack-an-api-and-get-away-with-it-part-1-of-3/

[15] http://www.zdnet.com/article/secret-tokens-found-hard-coded-in-hundreds-of-android-apps/

[16] https://www.washingtonpost.com/news/powerpost/wp/2016/09/12/thieves-stole-taxpayer-data-from-irs-get-transcript-service/

adequate security controls to protect sensitive, personally identifiable data. This option reinforces the need for a technology-neutral legislative approach and the setting of timelines once an adequate industry consultation process is complete.

4. An open banking regime should be designed around clear customer use-cases and pain points

Westpac's recommendations have been designed to address existing customer pain-points and use-cases. These include the following statements:

1) I want to easily compare products including pricing information (solved through standardised product reference data published via public APIs for ingestion by comparison websites and aggregators);

2) I want to easily share my transaction account and credit card transaction data with third parties (solved through a simple 'push' mechanism rather than the current mechanism available for customers to download/ upload CSV files through online banking or risk breaching terms and conditions by providing online banking credentials to third parties); and

3) I want to easily switch providers (solved by providing customers with the ability to manage and host data-sharing consents in one central place via a single interface, using a secure channel). For example, their online banking account, so that consents move across when the underlying account is switched.

5. Sharing of transaction account and credit card transaction data should be within scope of Phase Two

If the Government mandates the sharing of transaction data, Westpac has recommended that transaction data for both transaction accounts and credit cards form part of Phase Two. These two product types 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, 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 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 solved in the payments industry more broadly, with respect to the flagging and identification of recurring payments and direct debits. Currently, Westpac can only provide customers with a list of payments that we suspect are recurring payments or direct debits (as amounts to merchants may vary on a monthly or quarterly basis).

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 NPP.

While, we understand a mandated CCR regime is still under consideration, the Westpac Group is confident we could meet a late-2018 data supply requirement if this timing is mandated by the Government. NPP is in its final stages of testing and expected to move to Technical Go Live before the end of 2017. Following that milestone there will be a period of 'live proving' between

launch-ready participants, before the platform is opened up to support customer transactions in early 2018.

6. The sharing of personally identifiable customer transaction data in Phase Two should be based on a customer-centric design and informed consent

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.

In addition, it is important to maintain Australia's strong customer protection framework through an effective informed consent regime based on a customer's clear understanding of what data will be shared and how that data will be used by a third party.

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[17].

Westpac recommends the following principles be adopted:

- Opt-in and customer directed data sharing;
- Informed consent (customer knows exactly what they are consenting to, the scope of data to be shared, timeframes for transfer of data e.g. one-off or continuous and risks associated with data-sharing);
- Mechanism to control and protect customer privacy e.g. management of joint accounts;
- Standard set of consent types and wording;
- Easy 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).

In the UK ongoing customer permissioning will be left to the private market to determine e.g. individual bank permission dashboards or centralised permission management. As noted above, Westpac considers that online banking could provide a useful central consent dashboard.

7. Clear roles for Government, regulators and industry should be established

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;
- a *regulator* assumes primary responsibility for administering a data sharing licensing and accreditation regime, approving industry standards and protocols, and monitoring and enforcing industry compliance with those standards. In addition, accountability for

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

a consumer protection framework (which includes consideration of the need for customer recourse for losses) will need to be established. This could include discussion of a last resort compensation scheme for less-capitalised third parties; 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 technical data standards, protocols for safe data-sharing and governance and make recommendations on monitoring and enforcement and the development of a consumer protection framework. In addition, bilateral common participation agreements should be established between data providers and recipients.

8. A high-level legislative mandate should be established for open-data across the economy, encapsulated in a comprehensive access right to 'consumer data'. This could be achieved by leveraging existing legislation such as the *Privacy Act 1988.*

Westpac strongly agrees with the PC's recommendation that legislation can be used to provide clarity around the rules for improved data access, and can embed expectations on key issues such as effective risk management and the continuous endorsement of best practice as it emerges and develops.[18]

In our initial submissions to the PC, Westpac reflected on how the legal and regulatory framework in Australia is already evolving with the emerging data market and has clear scope to incorporate a more comprehensive data-sharing regime.[19]

Rather than passing new legislation for 'consumer data' and establishing enhanced customer rights in a segmented way (as the PC recommended), Westpac believes that the desired outcomes could be more effectively achieved by leveraging existing legislation (such as the *Privacy Act 1988*) to incorporate enhanced customer rights for data sharing.

Further detail on this approach is provided in Appendix 3.

Such an approach would enable permissive legislation to be economy-wide and create a consistent 'access right' across all industries, while industry specific data access principles and standards can ensure issues relevant to particular industries are captured. 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.

In addition, given the clear impetus for timely implementation, Westpac considers that incorporating the new consumer right under existing legislation and expanding an operative regulatory framework (e.g. through the Office of the Australian Information Commissioner (OAIC)) will deliver the most efficient and effective model for open data in Australia.

9. Permissive legislation should be technology neutral and should not mandate the method for data-sharing to ensure the regime can respond to future innovation

A technology neutral approach in legislation is essential given the real risks associated with identity theft, customer impersonation and breaches of data held by third parties are only likely to become clear once the regime is established and operational. For example, the legislation should not specify the use of APIs or authentication mechanisms.

[18] Productivity Commission Final Report (May 2018), *Data Availability and Use,* p 308.
[19] Westpac submission to the Productivity Commission, *Inquiry into Data Availability and Use* (22 August 2016), s 2.4.1, p 13.

The prescribed method of data-sharing in the UK via the use of public APIs has restricted the ability of members to respond to outstanding issues associated with authentication and verification, security, liability and fraud in the prescribed timeframes. These issues remain outstanding.

10. A strong and transparent open data governance regime must be established

A strong and transparent central governance regime should:

- Assist customers to recognise the value and sensitivity of data relating to their use of products and services (including the risks associated with data-sharing such as fraud and uncompensated losses);
- Allow customers to easily identify appropriately accredited and licensed third parties;
- Allow private sector organisations to protect their commercial-in-confidence / proprietary information; and
- Ensure data is shared in a secure environment supported by robust technical and security standards (particularly for financial information and other sensitive data) and compliance with existing privacy laws and confidentiality obligations.

Governance and regulation is essential to establishing trust and maintaining confidence. Previous research undertaken by the major banks suggests that Australia is starting from a relatively low level of customer confidence in data-sharing. As noted above, only 7% of Australians are comfortable with internet start-ups accessing their bank accounts to view transactions or transfer of money in/out[20].

In addition, enhanced data-sharing naturally increases the number of systemic risk factors that will need to be mitigated to ensure this fragile trust and confidence is not undermined, including large scale identity theft, cybersecurity attacks and a dramatic increase in fraud and uncompensated losses for customers.

Westpac considers there are three essential elements of a strong and transparent open data governance regime:

1. Accreditation and licencing;
2. Monitoring and enforcement; and
3. Consumer protection framework (complaints handling, external dispute resolution and compensation for losses)

The first two elements will require a central regulatory body to have responsibility for the data-sharing regime across the Australian economy. An objective accreditation and robust licensing regime is required to manage the appointment of data providers and recipients and, if necessary, the penalisation, suspension or removal of participants who do not comply with such requirements.

Combining these two roles under one regulator will help streamline the regulator's role in monitoring compliance and help minimise the resourcing uplift, while also reducing the burden on industry to report to multiple administrative bodies.

In addition, it will need to be determined whether responsibility for the consumer protection framework sits with the same regulator or a separate body.

[20] 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.

Consumer Protection Framework

A strong consumer protection framework should be comprised of:

- Complaints handling (including internal and external dispute resolution) for individuals and organisations (the need for a last resort compensation scheme should also be discussed);
- Clear liability standards;
- Sufficient measures to support customer redress and remediation in the event of unauthorised use or fraud;
- Mandatory breach notification requirement; and
- Requirements related to minimum capital, professional indemnity insurance etc. should also form part of the licensing and accreditation regime.

We expect a customer may attempt to look to the bank for remediation if:

- the data is not used by the third party data recipient in line with the customer's consent; or
- the data recipient has insufficient controls and safeguards in place for the protection of customer data, and the customer suffers identity theft, fraudulent activity or loss of funds as a result.

However, data providers will seek to be in no worse a position than today for customer data risks and liability. In particular, Westpac cannot be held responsible for the actions of a third party. If Westpac is compelled to provide a customer's data to a third party (at the customer's request), the bank cannot be held responsible for what happens to that data once it has been provided to the third party. The receiving party must take sole responsibility for using the data appropriately, in line with the customer's instructions and expectations, and keeping the data secure. The third party must therefore assume liability for any use (or misuse) of the data once it has been received.

In addition, 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.

There is the risk of a dramatic increase in fraud costs due to the combination of an enhanced data-sharing environment combined with the new instant-payment capabilities to be delivered by the NPP. A number of banks, including Westpac, currently offer customers relief from fraud losses arising from cybercriminal activity that is not triggered by the customer themselves. However, the increased exposure of customer-specific data (particular in an insecure environment – such as through the use of public APIs), creates an increased likelihood of compromise and instant settlement increases the consequences and potential losses for the customer (i.e. the money is 'gone' and the payment cannot be stopped). In the worst case, this could require the capping or removal of such guarantees by industry, with potentially catastrophic effects on some customers.

In 2016, Westpac compensated customers $57 million for fraud losses. We expect identity related loss events to rise under a regime where personal financial information is shared directly with third parties digitally (particularly in the absence of a clear liability regime as proposed above), 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 $89 million and $221 million for Westpac customers alone. The extrapolation of these losses across the industry suggest an inherent systemic risk across the banking system and industry. It also poses a risk to customers due to a possible lack of recourse to compensation and the rise of uncompensated losses thereby leading to broader costs to the Australian economy.

It is unclear whether third parties would have the capital to adequately compensate customers where they are liable for the data breach. 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. This reinforces why minimum requirements related to capital and insurance should form part of the licensing and accreditation regime. This may include the development of a new insurance market for data liability or cyber-insurance.

In addition, fraud risks are heightened as the payments environment moves closer to real-time. In Australia, the NPP enabling real-time payments will be operational in Australia from late 2017. This shift to real-time payments increases the likelihood that the money has gone by the time a fraud pattern has been detected. 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)[21]. In addition, the UK's customer guarantee and fraud policies are not as strong as current industry practice in Australia resulting in significant amounts of uncompensated losses for UK customers. The introduction of open banking in Australia, combined with real time payments, may therefore see actual losses accelerate above the UK's experience for the banks, customers and the economy.

As identity theft rates climb, banking security protocols may change to adjust for lack of both bank and customer confidence. This would typically involving reduced capabilities (e.g. daily payment limits) or higher-friction user experiences (e.g. more frequent two factor authentication of requests). This ultimately restricts the ability to meet customer needs and can result in a poor customer experience and outcomes. For example, in the UK, where identity theft rates are currently higher than Australia, if a customer fails their telephone banking credentials, many banks require the customer to visit a branch to prove their identity.

10. The remit of an existing regulator, preferably the OAIC, should be expanded e.g. the OAIC

In line with our recommendation to extend customer right under the *Privacy Act 1988*, Westpac's view is that the current remit of the OAIC should be extended to administer open data. This is preferable to establishing a new regulatory body.

The OAIC would be well-positioned to perform this governance role given its holistic coverage of both the public and private sectors across all industries. Although, it is noted a corresponding increase in resourcing would be required. In addition, the OAIC has a range of existing enforcement powers and remedies (including the ability to seek civil penalties) that may be

[21] https://www.pymnts.com/news/security-and-risk/2017/faster-payments-fraud-cybersecurity-biocatch/

relied and built upon in the context of a data-sharing framework. Similarly, existing OAIC initiatives such as 'Privacy Awareness week', guidelines and fact sheets could facilitate increased data literacy for individuals and the data-sharing community.

In relation to this governance role, Westpac considers the OAIC is preferable to ASIC (as the regulator should have responsibility for the economy-wide open data regime, not just specifically open banking) and the ACCC (as the Government's stated policy objectives are broader than a competition mandate).

11. The regulator should manage compliance with both economy-wide data standards and principles and industry specific data-sharing technical standards. Together, these should form the requirements for a new "Australian Banking Data Licence" and a whitelist of accredited participants.

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 strikes the right balance between making data-sharing easier and more accessible for customers while also ensuring all participants satisfy minimum privacy, confidentiality, consumer protection and data security requirements.

The prevalence of "ransomware" (malware which encrypts user's data and then offers to return it after payment) indicates the difficulty, in particular for small organisations, in protecting data. A recent industry study suggested that one ransomware gang alone netted US$325 million in payments from victims[22]. The Federal Government's Australian Cyber Security Centre saw a 300% increase in these kinds of ransomware attacks in 2015 over 2013[23]. The same report indicated that half of all respondents had experienced a cybersecurity incident in the preceding year.

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. While most banks have strong controls in place to protect against, and respond to, data breaches (as required by APRA and other regulators), newer players are unlikely to have as robust controls or response plans.

For example, small scale third party organisations do not currently have the scale or capital to implement bank-equivalent security protocols nor are they necessarily subject to stringent privacy and confidentiality regulation or minimum licensing requirements (data and security standards).

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. 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. 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.

[22] Source: https://cyberthreatalliance.org/pr/pr-102915.html
[23] Source: https://www.acsc.gov.au/publications/ACSC_CERT_Cyber_Security_Survey_2015.pdf

We believe this is best addressed through a licensing and accreditation regime comprised of:

- Economy-wide data standards;
- Industry specific standards; and
- Bilateral Participation Agreements.

A diagram of Westpac's proposed regulatory framework is in Appendix 4

This regime is not intended to create barriers to entry. To ensure the regime is not prohibitive to innovation and start-ups in Australia, the Government could consider a 'sandbox' approach under which partial relief from full licensing or endorsement standard criteria is provided for a one-off and narrowly defined period, for example, for pilot or testing (akin to ASIC's regulatory sandbox for fintech businesses).[24]

1. Economy-wide data standards (applied to public and private sector participants) to be captured in a "Code"

This would be an effective means of encouraging appropriate data-sharing conduct within a community of trusted users.

It is expected economy-wide standards should focus on the responsible use and management of data, including mandatory data and security breach notification requirements, accuracy, minimum data security requirements (including storage), transparency, safety, de-identification. The Data Governance Australia Code of Practice provides a useful example.

2. Industry specific standards to be captured in "Code Guidelines"

Industry specific standards (Code Guidelines) should cover:

- vetting of third parties;
- authentication/ verification;
- principles on liability allocation (including access and transfer);
- standard wording & protocols around informed consent;
- scope of data to be shared (e.g. transaction account/ credit card transaction history);
- appropriate timeframes (e.g. one-off use or alternatively ongoing permissions up to 12 months) and length of historical data required to be shared (e.g. last 12 months of transaction history);
- approved methods of data-sharing (public API platform for product reference and service data and an alternative, more secure, method for the sharing of personally identifiable transaction data to third parties);
- additional data security standards required to access personal, financial transaction data (including retention and destruction)data standardisation and data quality.

In addition, these Code Guidelines could cover specific standards around minimum capital and insurance requirements (including P&I), governance arrangements, requirement for security policies and procedures, complaints management (including internal dispute resolution and membership of an external dispute resolution scheme) and compliance with industry specific codes and legislation such as obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act.*

[24] See http://asic.gov.au/for-business/your-business/innovation-hub/regulatory-sandbox /

3. Bilateral Participation Agreements

Finally, bilateral participation agreements could be used to deal with particular issues between participants (data providers and recipients). This includes liability between participants (data provider and data recipient) during both the period of provision of data and the period following receipt of the data (which is no longer in the control of the data provider).

Standardised participation terms are particularly imperative in circumstances where a customer directs that information be shared with a third party that is not regulated under the Privacy Act 1988 (for example, if the Government does not legislate the comprehensive consumer right under the *Privacy Act 1988)* or otherwise does not operate under the same regulatory environment or standards as the disclosing organisation.

These agreements could also include 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 agreements will incorporate the Code and Code Guidelines by reference, ensuring rights and obligations are enforceable through contract law in addition to the overarching regulatory monitoring and compliance and consumer protection frameworks.

A whitelist approach

The licencing and accreditation regime supports 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.

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 un-authorised access, hacking and misuse.

For example, most banks use knowledge of account information and transaction activity to authenticate customers, including those who may have forgotten their password. A criminal (person or entity), could use fraudulently obtained customer information (including from a vulnerable third party), to transact on a customer's behalf (and transfer funds) or access additional information about the customer (e.g. current address information).

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 to ensure customers can distinguish between an appropriately accredited and licensed third party, and un-licensed players.

The standard setting process

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.[25]

Westpac strongly agrees that a regulator's approval of industry-devised standards is an effective means of consultation and will also support safe data-sharing from the bottom up. We note that industry codes of conduct already play an important role in regulating financial products and services in Australia.

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. This type of model could be seamlessly integrated into an Open Banking framework. RG 183 contemplates the appointment of a separate 'enforcer' or administrative body to monitor and enforce compliance with an approved standard. However, as noted above Westpac suggests that the appointed regulator for a data-sharing regime could play dual approval and enforcement roles.

Next Steps

Westpac welcomes the opportunity for further consultation with the Reviewer 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 a formalised industry working group process.

If you require any further information about this submission please contact Jade Clarke, Senior Manager, Government and Industry Affairs on jadeclarke@westpac.com.au or 02 8253 8492.

[25] PC Final Report, p 337.

Appendix 1: Outstanding issues in the UK

- ***Implementation of a customer protection framework***

No framework has been settled for the allocation of liabilities or payment of compensation where fraudulent or unauthorised access to data occurs (e.g. through phishing scams such as the recent Australian Taxation Office scam, where a customer inadvertently authorises a criminal to access their data, where a third party is hacked, or where data is transferred to an unauthorised third party due to customer impersonation or social engineering).

- ***Regulation and compliance***

It is not clear how third parties will be regulated to prevent criminals accessing data (e.g. creation of a whitelist), the registration and minimum governance requirements that will apply (e.g. in relation to data security), how monitoring and compliance of whitelist participants and overall governance of the system will operate, whether a new regulator should be established or the remit of an existing regulator should be expanded to step into this role and what funding would be required for compliance and enforcement activities.

Recent discussions suggest that a 'one stop shop' Licensing regime will be managed by the Financial Conduct Authority (FCA). However, monitoring and enforcement and the development of a customer protection framework have not been finalised i.e. enforcement and monitoring of individual participants and remedies.

The UK Implementation Entity has been established for the implementation and roll-out of the open data regime, and will not continue to exist beyond these activities (expected to be complete in 2018). Recent figures cited by the UK Implementation Entity suggest an annual budget of £70 million. Any new regulatory organisation will need to have a regulatory compliance and enforcement budget set appropriately and required on a continuing annual basis, which is expected to be significantly more than the Implementation Entity's current operating Budget.

- ***Interaction with competition legislation (conduct between participants)***

For example, whether a bank can temporarily or permanently revoke permissions to a given third-party application to access data while the regulator is determining an allegation of deliberate or accidental data loss or fraud.

- ***Vetting of third parties***

Challenges remain in relation to how banks will manage the vetting and authentication of third party requests and how terms of the access will be enforced.

In addition, Westpac understands that guidelines for consent, authentication/ verification and permission confirmation are in the process of being ratified.

Appendix 2: APIs

Westpac defines API categories in the following manner:

Private APIs	APIs that are used internally to Westpac, where other Westpac applications are the consumers of the APIs. Private APIs improve the agility for delivering change across the applications within Westpac, the use of Private APIs enable our multi-speed and multi-brand architecture.
Partner APIs	APIs that Westpac provide for Partners to exchange information or access functionality within Westpac. In the case of a Partner API there is an explicit arrangement (contract) between Westpac and the Partner which describes the obligations of the Partner and of Westpac.
Public APIs	APIs that Westpac provide for third parties to access Westpac information or functionality. In these arrangements all users of the API are covered by a standard Westpac contract, i.e. they are not individually negotiated with each party.
Open APIs	Are often considered as a variant on Public APIs. In the context of Open Banking APIs the key difference would be that neither the API nor the contract would be defined or controlled by Westpac.

It is worth noting that the cost of moving towards an API platform will be considerable, which the government should bear in mind in light of the already very substantial cost of changing regulation that the industry is currently absorbing.

Westpac does not currently have an API platform in place. Significant investment is required to develop our core functionality in this space, including for bilateral, partner APIs (i.e. an API set up directly between Westpac and another party which is underpinned by a legal contract). A bilateral API allows Westpac to undertake appropriate vetting of the third party, particularly given our existing legal obligations under the *Privacy Act 1988* and our duties of confidentiality.

We estimate the establishment of a basic API platform with foundational capabilities will cost Westpac approximately $25 million and take a minimum of two years to implement. Significant additional investment would be required for Westpac to move from basic API functionality to an open API platform capable of being accessed by any third party. For example, enhancements to existing security capabilities (estimated at $150 million). The ongoing maintenance, service and support of APIs (i.e., monitoring of performance levels and API version control) will create additional obligations and increased accountability and risk for an organisation to manage, resulting in extensive resourcing requirements and associated costs.

In their recent report, the House of Representatives Standing Committee on Economics ('the Committee') disagreed with the PC's preliminary view that implementing APIs would be prohibitively expensive. The Committee report has instead cited a figure of £1 million per institution in the UK for the 'development of an API framework from scratch'. In fact, the Committee has taken this figure from a report done by the UK Open Data Institute (ODI) and reflects the cost of the development of the policy.uk data portal which shares de-identified data through the website e.g. crime statistics. It is not, therefore, a comparable data point in considering the cost of developing APIs with material risk or security requirements.

The Westpac Group (Westpac) thanks the Committee for the opportunity to lodge a submission with the Inquiry. In addition, we endorse the submission lodged by the Australian Bankers' Association (ABA).

Appendix 3: Leveraging the *Privacy Act 1988*

Existing Australian privacy legislation creates a framework which, subject to limited exceptions, mandates the sharing of 'personal information' with individuals to whom the information relates.

The federal *Privacy Act 1988* also confers individual rights, including a right for the individual to request access to and correction of their personal information held by an organisation.

Organisations are required to respond to such requests within a reasonable timeframe, provide reasons where access is refused, and are entitled to charge a fee for access. The right of access to personal information held by a bank is exercisable by an individual that is a bank customer, including a business customer that is an individual conducting a business. The purpose or motive that the individual might have in wanting to access their personal information is not relevant. The right of access to personal information is exercisable against whatever entity holds personal information about an individual and so will not be affected by corporate structuring or sub-contracting.

In Westpac's view, enhanced consumer rights to data sharing could be incorporated as a new division under the Privacy Act (similar to, for example, the tailored consumer credit reporting provisions under Part IIIA). The objective would be to facilitate an efficient data sharing system while ensuring that the privacy of individuals is respected and the security of their information maintained. In recognition of that objective, the new provisions would intend to balance individuals' interest in protecting their personal information with the value of increased customer choice obtained via data sharing with approved third parties.

Appendix 4: Proposed regulatory framework