22 December 2016

Data Availability and Use
Productivity Commission
GPO Box 1428
Canberra City ACT 2601

**Supplementary Submission to the Productivity Commission**
**Data Availability and Use Draft Report**

The Westpac Group (**Westpac**) thanks the Productivity Commission for the opportunity to participate in the inquiry into data availability and use.

## EXECUTIVE SUMMARY

### Introduction

Westpac supports the development of an enhanced data-sharing regime in Australia. Data, when used effectively, provides immense value to businesses, governments, consumers and society in general.

We agree with the Productivity Commission's recommendation that consumers be given more control over data held about them through a new, overarching 'Comprehensive Right', while also allowing for the development of sector-specific standards for data-sharing.

However, the proposed definition of 'Consumer Data' in the Draft Report is very broad and could extend to any information held by an organisation from which an individual is identifiable or that is specifically linked to an identifiable individual (or that may be attributed to a particular customer). This will create some practical challenges for organisations to identify precisely what information would need to be provided to consumers. To ensure that the new 'Comprehensive Right' framework is both practical and implementable[1], we recommend the scope of the right and the definition of 'Consumer Data' are refined, to more appropriately strike the balance between the Productivity Commission's twin policy objectives of increasing trust and confidence in data-sharing while

[1] Draft Report page 345

also maintaining commercial incentives for organisations to invest in data collection and analytic capabilities[2].

Westpac recommends a principles-based approach to the new Comprehensive Right framework to ensure both consumers and organisations have requisite clarity as to what information must be provided to consumers under the new framework, in a manner that supports consumers' trust and confidence in the new regime.

A principles-based approach can be applied across different industries through the formulation of sector-specific standards, in a manner which allows relevant industry issues and exemptions to be dealt with, and will ensure the overarching framework is future-proofed and sustainable in an area of constant change and innovation. We welcome the opportunity to help develop such a principles-based approach.

The method for data sharing should not be mandated. Rather, a technology neutral approach is required to ensure sustainability of the framework over the long term. Data-sharing methods should be covered by sector-specific standards. As we outlined in our previous submission[3], 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 open or bilateral externally-facing application programming interfaces (**APIs**) and private marketplaces. Westpac believes that the financial services industry should develop common API standards and controls which should include an industry-wide cost model.

Westpac considers that the Government has a key role to play in increasing consumers' data literacy. We agree that ensuring trust and confidence in a data-sharing regime is essential, and that data breaches under the new regime could substantially undermine this objective being achieved. We consider that the establishment of appropriate safeguards is a fundamental requirement to assist the mitigation of these risks – particularly where sensitive consumer data is to be made available under the new Comprehensive Right. We believe that this is best addressed through a regulated data-sharing licensing regime based on minimum data governance standards that do not act as a barrier to entry.

Westpac's previous submission 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 consumer

[2] Draft Report page 13
[3] Pages 11 -13 of our previous submission

is shared with third parties. These issues will require further consultation before financial institutions are in a position to confidently share consumers' sensitive financial information with third parties. We are committed to working with both industry and Government to work through these issues.

We recommend that the Government adopt a phased approach to the regulation of shared financial information. This approach prioritises increasing consumers' access to data about themselves in a timely manner:

- Initially, financial information should be provided by financial institutions to their customers directly, using standardised data fields in a standardised form and useable format e.g. machine readable (this financial information may then be provided to a third party by the customer); and
- Following a period of industry consultation to identify solutions to address relevant privacy, security and liability issues, financial institutions should provide access to a consumer's financial information to third parties (at the customer's request and under an informed consent regime).

Westpac supports the Productivity Commission's acknowledgment that broader access to datasets in the 'national interest' will be an important component of a data-sharing economy. However, we strongly believe that datasets created and maintained by (and at the expense of) private sector organisations should only be nominated for release or sharing with 'trusted users' (as part of 'National Interest Datasets') on a voluntary basis, on terms that include appropriate provisions relating to security, confidentiality and liability and for reasonable compensation.

Finally, any timeframes should be appropriate to the Australian context. Westpac notes that market participants will require an adequate transitional timeframe to comply with any enhanced obligations due to the significant technology complexity and costs associated with increased data availability, access and use. We look forward to further consultation on these matters.

## Recommendations

A summary of Westpac's recommendations is below:

***Recommendation 1***: A moderated 'Comprehensive Right' and definition of 'Consumer Data' should be adopted, based on appropriate principles to ensure industry can develop compliant sector-specific standards and reduce the likelihood of organisations being disincentivised to invest in data capture and analytics.

***Recommendation 2:*** The method for data sharing should not be mandated. Rather sector-specific standards should provide clarity to consumers about the data they can expect to get about themselves by outlining *what* information would be made available to consumers and *how* that information would be made available.

***Recommendation 3:*** The Government should adopt a phased approach to the regulation of shared financial information. Phase one should prioritise consumers being given access to their financial information in a standardised and useable format. Access to consumer information should subsequently be granted to third parties (with the consumer's consent), once additional privacy, security and liability concerns have been addressed.

***Recommendation 4***: To limit risks and enhance trust and confidence in data sharing, the release of data to third parties should be as directed by the consumer and limited to disclosure to 'trusted' or 'accredited' third party users. A new regulated licensing regime should require entities to meet certain baseline governance standards for sharing (and receiving) data. Government also has an important role to play in educating consumers about the value of their data, including about the risks of data sharing.

***Recommendation 5:*** For the banking industry, an industry-led working group should develop a set of common API standards and controls applicable to the financial services industry. These would include agreement on the standardisation of datasets, codification of non-negotiable API security requirements, interface definitions and specifications, responsibility for the data and service levels and standards.

***Recommendation 6***: The industry-led working group should detail the cost implications of industry-standard APIs and formulate an appropriate industry-wide cost model.

***Recommendation 7***: The nomination of private sector datasets for release or sharing (as part of National Interest Datasets) should only occur on a voluntary basis, where there is reasonable compensation for the data owner and on terms that include appropriate provisions relating to security, confidentiality and liability.

## SECTION 1: Consumer Rights

### 1.1 Introduction

We are broadly supportive of the Productivity Commission's proposed data-sharing framework, under which consumers would have a 'Comprehensive Right' to access their 'Consumer Data'.

However, the scope of the information that may fall within the proposed definition of Consumer Data in the Draft Report is too broad and could extend to any information from which an individual is identifiable or that is specifically linked to an identifiable individual. As currently drafted, we believe that it will be challenging for organisations to identify precisely what information would need to be provided under this new Comprehensive Right. These challenges are outlined further below.

It is essential that the Productivity Commission's objectives to increase trust and confidence and preserve commercial incentives to collect and add value to data are both achieved under a new regime.

We agree that, to be effective, both the Comprehensive Right and the definition of Consumer Data need to be 'practical and implementable'[4]. In particular, we believe it is essential that both consumers and organisations have clarity as to the scope of information that consumers (and their nominated third parties) should have access to under the Comprehensive Right.

In particular, the Comprehensive Right should:

- Assist consumers to recognise the value of data relating to their use of products and services;
- Allow private sector organisations to protect their commercial-in-confidence / proprietary information;
- Ensure data is shared in a secure environment through robust security standards (particularly for financial information and other sensitive data) and compliance with all privacy laws and confidentiality obligations; and
- Maintain Australia's strong consumer protection framework through an informed consent regime based on a consumer's clear understanding of what data will be shared and how that data will be used.

[4] Page 345 of the Draft Report

We recommend the Comprehensive Right is moderated by the following set of basic principles which, when taken together, can achieve these objectives.

### 1.2 Basic principles for implementing the Comprehensive Right

We acknowledge that organisations in different industry sectors will hold different types of data about their customers; however, we believe that the basic principles outlined below could be applied to all industry sectors and reflected consistently in industry standards to implement the new data-sharing regime.

These principles are consistent with the framework under the *Dodd-Frank* legislation in the US which permits consumers to access information relating to their use of financial products and services[5].

- ***Principle 1:*** *The information to be provided must relate to the consumer's use of products and services*

  A consumer's right to access 'Consumer Data' should only extend to information that relates to that person in their capacity as a consumer (i.e., the information should relate only to their use of products and services provided by the relevant organisation).

  Organisations may hold information about their customers in other capacities, for example, because of an employment or supplier relationship, which should not fall within the scope of this new right to access 'Consumer Data'.

  Better defining the scope of the Comprehensive Right so that it is more clearly aligned to a person's capacity as a consumer would also limit unnecessary overlap or confusion with an individual's existing broad rights to access 'personal information' under the privacy regime. To the extent that individuals wish to access information that does not relate to products or services provided by the organisation to them in their capacity as a consumer, making a request under the privacy regime would continue to be the most appropriate avenue to obtain access.

  Overall, the framework should not be used to create a reporting or data information service.

[5] Section 1033 (Consumer Rights to Access Information); Dodd-Frank Wall Street Reform and Consumer Protection Act 2010

- ***Principle 2**: Organisations must not be required to disclose any commercial-in-confidence / proprietary information or any sensitive information to consumers or their nominated third parties*

  It is essential to preserve commercial incentives for organisations to collect and add value to data – this was one of the key factors considered by the Productivity Commission when assessing options for improving data availability and use[6]. We strongly believe that commercial-in-confidence / proprietary information should not form part of the Comprehensive Right. Rather, it should be shared with third parties on a voluntary basis, in a secure and controlled manner and on commercial terms through the use of private marketplaces and bilateral arrangements. We consider this will better support the Productivity Commission's objectives to maintain investment, innovation and competition in the market.

  As an example, any derived customer insights and measures, including the outputs of models and other calculations – in which organisations make considerable investments in order to develop tailored and competitive services – should be expressly out of scope for mandated sharing, as these constitute core commercial and competitive assets of participating organisations. Westpac would also not be willing to share commercial-in-confidence information generated for use as part of its internal business decisions, such as credit, risk or other rating models, assessments or profiles relating to customers or details of commercial decisions that Westpac has made as to whether or not to offer credit or other financial products to its customers.

  In addition, there are certain types of sensitive information that it 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:

  - Westpac would never disclose a customer's online banking or other passwords to the customer (or third party), even in response to a direct request from the customer, due to the risk of fraud / unauthorised access to the customer's accounts;
  - Similar risks also exist in relation to the provision of certain identifying information, such as the customer's date of birth or passport / drivers' licence details, to a third party; and

[6] Page 295 of the Draft Report

- Financial institutions collect sensitive information about customers to meet regulatory requirements, for example, information for the purposes of monitoring or reporting financial crimes or suspicious transactions, which by law must not be shared with the customer.

It is therefore appropriate that categories of data, such as these, are carved out from the Comprehensive Right under this principle.

- ***Principle 3****: The information must be reasonably retrievable by the organisation in the ordinary course of its business*

  This principle is essential to ensure that, from a practical perspective, organisations are able to manage data requests from consumers (and their nominated third parties) in an efficient and timely way and are not required to undertake onerous 'data hunting' exercises to locate information that the data holder may not be able to retrieve in the ordinary course of its business.

- ***Principle 4:*** *Organisations must have an appropriate level of confidence that information is accurate and relates to the consumer*

  While organisations may have a high degree of confidence that certain data they hold about consumers is both reasonably accurate and does in fact relate to a particular consumer (for example, where the data relates to transactions made by a customer where their identity has been confirmed), there are other categories of data in which the organisation may have a lesser degree of confidence about the accuracy of the information or where the organisation assumes (but has not verified) that the information relates to a particular customer.

  For example, organisations usually hold information about a person's internet browsing history based on an 'internet protocol' address which identifies a particular device used to access the internet (rather than identifying the user of that device). Given a device, by its nature is not necessarily personal and there is the potential for multiple users, it is not possible to identify which user the browsing history relates to. We believe that providing this information to a particular consumer is problematic as it may result in a person's privacy being breached (for example, where the recipient of the information is not the user but can deduce who the actual user of the device is).

Similarly, the provision of inaccurate information to a consumer (or their nominated third party) may also be problematic and may result in liability and / or reputational harm for the disclosing organisation.

***Recommendation 1***: A moderated 'Comprehensive Right' and definition of 'Consumer Data' should be adopted, based on appropriate principles to ensure industry can develop compliant sector-specific standards and reduce the likelihood of organisations being disincentivised to invest in data capture and analytics.

### 1.3 The role of sector specific standards

Westpac supports the Productivity Commission's view that industry sectors are best placed to set standards of data transfer for effective data-sharing.

We propose that scalable industry-specific standards should be developed through industry consultation to distinguish between, and appropriately manage, the differential risks associated with different industry datasets and allow relevant industry issues and exemptions to be dealt with in a compliant manner.

For example, the financial services industry and other industry sectors would determine standards that would outline:

- *What information would be made available to consumers in that sector*

  This would need to have regard to the consumer's use of relevant products and services in each industry sector. Although we expect that the information types may differ across different industry sectors, we believe the principles outlined above could be applied in all sectors.

- *How that information would be provided to customers*

  The information would need to be provided in a standardised form by way of common content and data structures across each industry and provided in a format which is consistent across the relevant industry and useful for customers.

The method for data sharing should not be mandated by Government. Rather, data-sharing methods should be covered by sector-specific standards under the new Comprehensive Right regime. A technology neutral approach is required to ensure sustainability of the framework over the long term.

***Recommendation 2***: The method for data sharing should not be mandated. Rather sector-specific standards should provide clarity to consumers about the data they can expect to get about themselves by outlining *what* information would be made available to consumers and *how* that information would be made available.

### 1.4 A phased approach to data sharing

Westpac supports an enhanced data-sharing regime which would include sharing data with third parties that are appropriately authorised by customers and that comply with minimum data governance standards. As previously noted, sharing a customer's financial or other sensitive information with third parties involves greater privacy, security and liability concerns than where this data is provided directly to customers (who may then elect to pass that information to third parties, for example to obtain offers of products or services from a competitor or to use a product comparison service).

Financial institutions are required to take reasonable steps to maintain accurate and up to date data. What is reasonable will depend on the circumstances. Where an institution controls its own use of data, and has its own checks and balances on how the data is used, that will inform the extent of efforts required to ensure that information is accurate and up to date. A requirement to release information to third parties who may not have the same checks and balances (or who may not use the information for the same purposes) should *not* expose the disclosing organisation to additional requirements around the way the data is managed. Nor should the disclosing organisation be liable for the fitness for purpose of the information in a mandatory data-sharing environment – this must be the responsibility of the recipient.

Our previous submission[7] outlines a number of potential difficulties where data is to be shared with third parties, including:

- in verifying the third party's identity;
- the need to manage customer consents in a way that is both practical (from an operational perspective) and allows the institution and customer to keep track of the scope and validity of consents (which may relate to multiple third parties). There would be additional complications where, for example, the customer holds an account jointly with another person; and
- additional data security risks, where the third party does not maintain equivalent or higher standards and safeguards to the disclosing organisation.

[7] Pages 9 – 11 of our previous submission

There are also questions of liability in the context of the issues outlined above and in our previous submission. Although the disclosing organisation will no doubt still be at risk from a reputational perspective, any regime which requires data to be shared must ensure that the recipient of the relevant data assumes all liability for use or misuse of the disclosed information.

There are many different aspects to be considered here. Given the sensitivity of banking information relating to a customer, we believe that these important issues require further consideration and industry consultation before financial institutions are in a position to confidently share sensitive information relating to their customers with third parties (with the customer's consent). We are committed to working with both industry and Government to work through these issues.

We also recommend that the Government adopt a phased approach to data-sharing, which prioritises increasing consumers' access to data about themselves in a timely manner:

- Initially, financial information should be provided by financial institutions to their customers directly, using standardised data fields in a standardised form and useable format e.g. machine readable (this financial information may then be provided to a third party by the customer); and
- Following a period of industry consultation to identify solutions to address relevant privacy, security and liability issues, financial institutions should provide access to a consumer's financial information to third parties (at the customer's request under an informed consent regime).

***Recommendation 3***: The Government should adopt a phased approach to the regulation of shared financial information. Phase one should prioritise consumers being given access to their financial information in a standardised and useable format. Access to consumer information should subsequently be granted to third parties (with the consumer's consent) once additional privacy, security and liability concerns have been addressed.

### 1.5 Increase consumer data literacy

Consistent with our previous submission, we believe that the Government and industry can play a major role to increase data literacy across Australia. We believe that increasing consumer data literacy will foster more effective and extensive adoption of the new data-

sharing framework and we support the Productivity Commission's proposal that consumers should be educated by relevant regulatory bodies about their rights under the new regime[8].

This education must include raising awareness of the risks involved for consumers if they elect to share data with third parties, to ensure that consumers can make genuinely informed decisions about the use of their data. We provide further comments on the need to make customers aware of the risks and implications of sharing their sensitive financial information with third parties in section 2.1 below.

[8] Draft Recommendation 9.3

## SECTION 2: Data sharing standards and use of APIs

### 2.1 Data-sharing licensing regime

In our previous submission, Westpac noted the fundamental importance of an appropriate licensing regime being implemented as part of an enhanced data access regime. We also noted that the Government has an important role to play in increasing consumer and industry confidence in data-sharing by introducing a data-sharing licensing regime for all market participants, to be overseen and administered by an appropriate regulatory body[9]. This would involve minimum governance standards that apply across all industries (both public and private sectors) and would be an effective means of encouraging appropriate data-sharing conduct within a community of trusted users.

In particular, financial services providers and other industries that hold sensitive data sets will need to have confidence that third parties seeking to access that data (with the customer's consent) will, at a minimum, be able to manage and maintain this type of data securely and respectfully.

Given the serious consequences that can occur when financial or other sensitive information is not kept securely and managed appropriately, it must be made appropriately clear to any customer wishing to permit a third party to access their financial information that:

- the integrity of any third party which the customer authorises to access their data cannot be guaranteed (even if that third party meets the minimum standards referenced above);
- the transferring organisation is not liable for any use (or misuse) of that data by the third party (or other parties who subsequently receive or gain access to the data after it is provided to that third party); and
- therefore, the customer should only provide access to third parties that they trust, having done their own due diligence.

***Recommendation 4***: To limit risks and enhance trust and confidence in data-sharing, the release of data to third parties should be as directed by the consumer and limited to disclosure to 'trusted' or 'accredited' third party users. A new regulated licensing regime should require entities to meet certain baseline governance standards for sharing (and receiving data. Government also has an important role to play in educating consumers about the value of their data, including about the risks of data-sharing.

9 Page 16 of previous submission

This approach is consistent with that proposed by the Open Banking Working Group in the United Kingdom where it has been acknowledged that a vetting process is a reasonable precaution to take when dealing with financial data[10].

It is not intended that a data-sharing licensing regime would create a barrier to entry for non-bank entities. Westpac maintains that it would be appropriate for Government to consider adopting a (strictly time bound) 'sandbox' approach for new entrants to pilot or test their market offering without the need to complete the full licensing and accreditation process.

## 2.3 The use of APIs

### 2.3.1 By third parties (with the customer's consent)

The Productivity Commission has requested further information on the benefits and costs of providing data using APIs. We reiterate that, in addition to APIs, there are other ways in which information can be shared between organisations and their customers (and with their nominated third parties) effectively and securely. Therefore, we do not believe that the Government should mandate the use of specific mechanisms for data-sharing. This will ensure the framework is flexible, sustainable and is sufficiently future-proofed to allow for future innovation in data-sharing mechanisms.

Consistent with our previous submission[11], Westpac believes that the use of externally- facing APIs to transfer financial information to third parties would present significant challenges. In particular, we believe that a number of key risks associated with the use of APIs (which include cyber security, customer identity verification and authentication) would be heightened when APIs are used to transfer large quantities of data about individual customers between banks and non-bank entities (which often have different security standards). These risks may not be widely or fully understood.

Consequently, the sector-specific working groups should address mechanisms for sharing data, including APIs. If designed, operated and managed appropriately, Westpac considers that APIs can provide efficient data access and security controls to enable effective data transfers between organisations and that many of the risks associated with the use of APIs can be managed through increased technology and non-technology controls.

10 ODI and Fingleton Associates (Open Data Institute and Fingleton Associates) 2014, Data Sharing and Open Data for Banks, A report for HM Treasury and Cabinet Office, UK Government, London, UK. 2016, p. 3 and is also referenced on page 555 of the Draft Report.

11 Refer to previous Westpac submission pages 9 to 12.

We believe that there would be great benefit in industry working groups developing common API standards and controls, including consideration of similar initiatives relating to the use of APIs that are in place or being developed overseas.

***Recommendation 5***: For the banking industry, an industry-led working group should develop a set of common API standards and controls applicable to the financial services industry. These would include agreement on the standardisation of data sets, codification of non-negotiable API security requirements, interface definitions and specifications, responsibility for the data and service levels and standards.

The working group should, as a starting point, consider whether the standards being developed overseas, such as OpenID[12], OAuth2[13] and the Open Banking Standards[14] in the United Kingdom (and any lessons from those initiatives), can be appropriately applied to the financial services industry in Australia to mitigate the heightened risks arising from the use of APIs. This would include assessing the merits of adopting possible solutions such as OAuth2 and the Open Banking Standards to authenticate customers through each bank's own online banking platform as part of the API data transfer process and to manage customer consents.

### 2.3.2 With consumers

Due to the technical requirements to set up and maintain APIs, we do not consider that APIs would be appropriate for use between Westpac and its retail and small business customers. We believe that information is best made available for access and download by our customers directly through our online banking platform using downloadable and machine readable data files (e.g. CSV files).

## 2.4 Cost of APIs

We note that the Productivity Commission refers to a study which estimates the cost of API implementation (in the United Kingdom) to be one million pounds[15]. Although Westpac has not fully costed the implementation of a suitable API platform, our high-level estimate for putting in place and maintaining an externally facing API solution to support the anticipated

[12] OpenID allows you to use an existing account to sign in to multiple websites, without needing to create new passwords. http://openid.net/

[13] OAuth is an open standard for authorisation, commonly used as a way for Internet users to authorise websites or applications to access their information on other websites but without giving them the passwords

[14] Open Banking Standards as part of the Open Data Institute: https://theodi.org/open-banking-standard

[15] Page 556 of the Draft Report

scale of the proposed Comprehensive Right is significantly higher than the Productivity Commission's estimate.

In estimating costs we note that both the upfront cost and the cost of continued investment to implement, monitor and maintain robustly secure and effective API services need to be taken into account, as well as the costs of implementing and maintaining an accurate and secure consent management framework (where data is to be shared with third parties).

***Recommendation 6***: The industry-led working group should detail the cost implications of industry-standard APIs and formulate an appropriate industry-wide cost model.

As a starting point, Westpac suggests a possible commercial model would entail charging a reasonable service fee for each instance of third party access to the bank's systems to receive (and subsequently commercialise the use of) data about an individual customer (with the customer's consent).

This model would preserve financial institutions' commercial incentives to invest in the implementation and maintenance of APIs through which a third party is able to access (and commercialise) a customer's information (with the customer's consent). Any such fees would be regulated by market forces and by the Australian Competition and Consumer Commission.

## SECTION 3: National Interest Datasets

### 3.1 New access framework

We support the Productivity Commission's proposed framework to enable wider access to certain high-value National Interest Datasets[16] and agree that the framework needs to take account of the significant differences in data types and associated risks[17].

This must include consideration of the value of the data, particularly when the data has been created and maintained by (and at the expense of) private sector organisations which have made substantial investments in their data collection, storage and analytics capabilities.

### 3.2 Private sector datasets

To ensure that the private sector retains incentives to invest in data collection and analytics, it is essential that the Productivity Commission clarifies the circumstances in which private sector datasets may be nominated as National Interest Datasets (and assessed as suitable for release to the public at large or to 'trusted users').

Westpac believes that private sector datasets should only be nominated for release or sharing with 'trusted users' in the following circumstances:

- **on a voluntary basis** – private sector data holders must be able to make a commercial decision as to which of their datasets (if any) they wish to nominate for release, taking account of factors such as the value of the data to their business, the costs incurred in collecting or adding value to the data, and any barriers to release (for example, restrictions in contractual arrangements or concerns around liability);
- on terms that include appropriate provisions relating to **security, confidentiality and liability** where necessary (having regard to the nature of the dataset and the risks or potential liability associated with release); and
- **for reasonable compensation** – we agree that appropriate incentives will be needed if private sector data is to be contributed as part of National Interest Datasets[18]. Compensation for the data holder may take a number of different forms, including the purchase of a private sector dataset by Government on

[16] Draft Recommendations 2.1 , 9.4 and 9.11
17 Page 339 of the Draft Report
[18] Page 379 of the Draft Report

commercial terms or through the data holder charging users for access to the dataset.

The designation of private sector datasets for release without the data holder's consent or without appropriate compensation would be inconsistent with one of the Commission's key criteria –namely, the need to preserve commercial incentives to collect and add value to data[19]. We strongly agree that protection of commercial-in-confidence / proprietary data is an essential underpinning feature of competitive markets.

***Recommendation 7***: The nomination of private sector datasets for release or sharing (as part of National Interest Datasets) should only occur on a voluntary basis, where there is reasonable compensation for the data owner and on terms that include appropriate provisions relating to security, confidentiality and liability.

### 3.3 Data collected by financial institutions

In our previous submission we:

- outlined how Westpac currently provides information to our customers to support them to make informed decisions;
- set out our proposals for information to be provided to individuals and their nominated third parties in a consistent and standardised form to promote ease of comparability and customer choice;
- noted Westpac's investment to foster and grow its data analytics and data management capabilities, to derive insights to support informed business decisions and improvements to customer service; and
- outlined how Westpac participates in data-sharing marketplaces that involve sharing data through exchange platforms which are subject to robust security controls.

We do not agree with the suggestion that financial institutions should be subject to a higher obligation to make data available to the public or to third parties than other organisations operating in less regulated sectors. We believe that this suggestion is inconsistent with the Productivity Commission's recognition of the need to preserve commercial incentives to collect and add value to data. We also reiterate that established organisations should not be expected to subsidise new market entrants in data-sharing initiatives.

[19] Page 295 of the Draft Report

### 3.4 Data collected for regulatory reporting

The Draft Report suggests that data collected by financial institutions in the course of meeting regulatory requirements could form part of a National Interest Dataset[20] (and therefore be released by regulators as part of the new framework).

We would need to consider the implications of this on a case-by-case basis in light of:

- the extensive and varied datasets that we currently provide to regulators (both as required by law and on a voluntary basis); and
- the likely expansion of regulatory reporting obligations over time. In particular we note that there is a trend for regulators to seek more granular data from financial institutions and regulators are themselves investing heavily in data collection and data analytics capabilities.

We therefore believe that further consultation is necessary before any obligation to release datasets that are provided by organisations to regulators is introduced. For example, there are a number of important issues that require consideration such as:

- whether the release of the data may result in detriment to the commercial interests of the organisation that has collected the data and / or other organisations to which the data relates (for example, customers or market participants);
- whether any part of the information is attributable to a particular financial institution or whether it would be possible to identify or infer the identity of the financial institution or any third parties (either from the relevant dataset or through combining the information with other datasets);
- for any proposal to release data that relates to individuals or other organisations; the privacy constraints and any consents required from the parties involved;
- whether certain types of commercial-in-confidence / proprietary or sensitive data may not be suitable for release (even on an aggregated or de-identified basis), such as privileged information, competitively sensitive information and / or data relating to financial crimes / suspicious transaction reporting; and
- whether the data has been provided to the regulator on a standardised and consistent basis by different organisations – if this is not the case then it may result in commercial detriment to organisations (where comparisons are made on the basis of inconsistent data) and may also be of limited use.

[20] Pages 264 and 356 of the Draft Report

### 3.5 Contracting with Government entities

The Draft Report recommends that Government bodies retain the right to access or purchase data that is created in the course of contracting with the private sector for the delivery of public services[21].

We note that these rights to access or purchase data would need to be negotiated with private sector counterparties on a case-by-case basis and that this may result in lengthy contractual negotiations. In particular, we expect that there will be additional complexity when the relevant data created is subject to privacy or confidentiality obligations or when there are multiple service providers or multiple parties seeking to assert rights over the relevant data.

[21] Draft Recommendation 4.2

**SECTION 4: Comprehensive credit reporting**

Westpac considers that competitive forces, rather than mandating, should shape Comprehensive Credit Reporting (CCR) in Australia. However, we recognise that a mandated regime may be considered by Government if a minimum level of voluntary participation is not achieved in the future. We recommend that industry and Government continue to discuss an appropriate review period and thresholds around minimum participation levels.

Westpac has invested, and will continue to invest, in robust data management processes to enable compliant sharing and receipt of credit data. Westpac has progressed towards pilot testing the requirements of CCR with our credit bureaus and we are continuing to develop our technical capability to facilitate the achievement of this milestone. Some CCR issues remain outstanding, for example, hardship reporting. Westpac is working actively with industry and other stakeholders to resolve this issue.