CUSTOMER OWNED BANKING ASSOCIATION

www.customerownedbanking.asn.au

LEVEL 11, 35 CLARENCE STREET, SYDNEY NSW 2000 GPO BOX 4686, SYDNEY NSW 2001

Ms Roslyn Bell
Data Availability and Use Inquiry
Productivity Commission
Canberra ACT 2601

Via online: www.pc.gov.au/inquiries/current/data-access

Dear Ms Bell

Productivity Commission Inquiry into Data Availability and Use

The Customer Owned Banking Association (COBA) welcomes the opportunity to comment on the Productivity Commission Issues Paper *Data Availability and Use*.

COBA is the industry association for Australia's customer owned banking institutions, i.e. mutual banks, credit unions and building societies. Collectively, the sector we represent has $99 billion in assets and provides the full range of retail banking products to more than 4 million customers.

The customer owned model is the proven alternative to the listed model in the Australian banking market, delivering competition, choice, and consistently market leading levels of customer satisfaction.

Customer owned banking institutions are:

- Public companies structured under mutual ownership principles set out in ASIC Regulatory Guide 147 *Mutuality – Financial institutions*;
- Authorised Deposit-taking Institutions (ADIs) regulated by APRA under the *Banking Act 1959*;
- Australian Financial Services Licensees regulated by ASIC under the *Corporations Act 2001*;
- Australian Credit Licensees regulated by ASIC under the *National Consumer Credit Protection Act 2009;* and
- Reporting entities regulated by AUSTRAC under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006.*

Banking institutions rely on access to data and capacity to analyse and report data for their commercial operations and to meet a wide range of regulatory obligations. Banking institutions are trusted custodians of customer data and are strongly committed to the highest levels of protection of customer data.

COBA notes that the Government requested the Productivity Commission (PC) to undertake this inquiry in its policy statement on FinTech and in response to recommendation 19 of the Financial System Inquiry (FSI).

COBA supports well-considered measures that promote innovation to improve consumer outcomes and competition. Customer owned banking institutions are committed to innovation as a means of delivering value for customers. For example, COBA members have entered into strategic partnerships with FinTechs and are ahead of three of the four major banks in making Android Pay available to customers.

The key issues for the customer owned banking sector under consideration by the PC in this inquiry are:

- mandatory participation in comprehensive credit reporting (CCR);
- the use of open Application Programming Interfaces (APIs) so that customers can share their account data with third parties; and
- access to Government data sets.

CCR

COBA's preference at this time remains that participation in CCR should remain voluntary. There are mixed views in our sector on this question, with some COBA members seeing merit in moving to mandate participation by larger lenders.

If, in the future, the Government decides to mandate participation in CCR by credit providers, it should only be made mandatory for lenders large enough to make a material difference to the value of the database. We suggest a threshold of lenders with assets of more than $200 billion or with more than 1 million customers. There is no compelling case, on a cost-benefit basis, for mandating participation by small lenders.

Access to customer data

COBA supports increasing capacity for fully-informed, consenting consumers to access and share data about themselves with trusted third parties.

The current method some FinTechs use to access customer data is highly problematic. Problems of security, liability for fraud, and risk need to be addressed to allow the adoption of common or standardised Application Programming Interfaces (APIs), referred to as "Open APIs", [1] to drive innovation, competition and consumer choice. Allocation of costs and cost-recovery is also a factor that must be addressed in any new framework.

One possible solution for resolving these issues is to establish a voluntary, co-regulatory regime requiring all entities wishing to access ADI account data under an open API regime to meet minimum probity and competence requirements, and comply with a business-to-business code of practice. Such an approach will establish a common platform enabling consumers to safely and securely share their account data with trusted third parties. For example, consumers could use their transaction data to get a comparison of credit cards from different providers that is tailored to their individual patterns of use.

Government databases

ADIs should be allowed, where appropriate and subject to a strict consumer protection framework, to use Government databases to meet regulatory obligations, such as verification of customer identity. We note that use of Government databases does not necessarily require access to these databases.

Comprehensive Credit Reporting

COBA's long-standing position on CCR is to support voluntary participation in CCR. At this time this remains COBA's preference. We note that the PC is examining the "uptake of the credit reporting framework" and will "consider recommendations for improving participating in such initiatives".

The FSI recommended support for industry efforts to expand credit data sharing under the new CCR regime. FSI Recommendation 20 went on to say: *If, over time, participation is inadequate, Government should consider legislating mandatory participation.*

The FSI noted that significant portions of credit data will not be exchanged until late 2016 or early 2017 and that in 2017, Government "should review industry's

[1] Our use of the term 'Open API' refers to a common language for an application programming interface that would provide programmatic access to a proprietary software application (in this case, FinTech access to customer data held by an ADI). We do not take it to mean the same as 'open data', which allows unrestricted access and use of customer data held by an ADI.

participation in CCR to determine whether a regulatory incentive or legislation for mandatory reporting is required."

This is an appropriate timeframe for considering further action in relation to CCR.

While CCR has theoretically been possible since changes to the Privacy Act in 2014, industry has been awaiting finalisation of the Principles of Reciprocity and Data Exchange (PRDE), the industry developed framework governing the exchange of positive credit information. The ACCC gave approval to the PRDE in December 2015, providing greater certainty for industry.

As at October 2015, 25 lenders were reportedly[2] contributing positive data to credit bureaus, including one major bank, and there were 7 million accounts with CCR records, or 24 per cent of accounts in the retail credit market with CCR data.

Despite this, COBA understands there has been very limited exchange of positive information since the ACCC authorised the PRDE. The majority of lenders that are contributing data are doing so in 'private' mode, with very few lenders exchanging data. The reasons for this poor level of participation include competitive and strategic positioning by large players, cost factors, and unresolved issues and uncertainty about the application of CCR.

For example, there is an unresolved issue relating to how repayment history information (RHI) is reported for customers in hardship. In particular, in cases where a customer and lender have come to a 'simple arrangement'[3] but the customer's contract has not been formally varied. This issue could be resolved by a legislative change to allow for a 'hardship flag' to appear on a customer's credit report in relation to the above scenario. This is the optimal solution to protect the accuracy and integrity of the credit reporting system and the interests of customers in hardship situations.

Several COBA members have made investments in CCR and these members will only realise the necessary return on their investments when participation reaches a 'tipping point'. International experience shows that the 'tipping point' is reached when there is more than 40% of participation in CCR. In Australia, this tipping point will only be reached when the largest market participants are contributing and exchanging data.

COBA is sympathetic to calls by the FinTech lobby to mandate participation in CCR[4]. However, COBA is also concerned that mandating participation for all credit providers will come at too high a cost compared to the benefits. Based on data provided by COBA members, the cost of implementing CCR is between $400,000 to $1 million for an individual ADI. For many COBA members, this is cost prohibitive and other solutions will have to be found over time. There are more than 60 customer owned banking institutions each with total assets of less than $1 billion.

Some lenders are concerned that, at this stage, the potential benefits of participating in CCR are outweighed by the cost of transitioning to CCR. For these reasons COBA continues to support voluntary participation but if mandated participation is to be considered, it should involve a threshold to ensure the appropriate cost-benefit balance. In our view, mandated participation should not apply to ADIs with assets of less than $200 billion or less than 1 million customers.

COBA suggests this threshold because lenders with assets of more than $200 billion currently hold 77.3% of the mortgage market and 72.6% of the total lending market in Australia, which represents the vast majority of customer accounts about which positive data might be reported.[5]

If participation in CCR was made mandatory for the largest lenders, international experience suggests that mid-tier players would face strong incentives to participate

[2] Shaun Drummond, Australian Financial Review, 29 October, 2015: Veda chief talks up 'positive' credit reporting.
[3] A simple arrangement is defined in ASIC Class Order [CO14/41], which allows credit providers to enter into a simple arrangement with a customer, which is defined as 'an agreement that defers or reduces the obligation of a debtor for a period of no more than 90 days'.
[4] FinTech Australia position paper '*Priorities for reform of the Australian Financial Services Industry*', released February 2016
[5] Source: APRA, RBA. Figures correct as at March 2016.

because the value of participating and the opportunity costs of not participating at that point would increase.[6]

There is no compelling case for mandating CCR for smaller lenders, because their cost of transitioning would be disproportionately high and the value of their data would not be significant in delivering the wider benefits of CCR.[7]

If the Government decided to mandate CCR for the largest lenders, it should be done with a transition period of at least 18 months.

Consumers' access to, and control of, data about themselves

COBA notes that the terms of reference of the Inquiry includes identifying options to improve consumers' access to data about themselves and to examine the benefits and costs of those options.

In principle, a consumer's data belongs to the consumer and consumers have the right to access, and control access to, data about themselves.

This right needs to be balanced by consideration of factors such as ensuring full-informed customer consent, maintaining security and integrity of data, cost and competitive impacts.

Debate about consumers' access to, and control of, their own data held by ADIs is acutely relevant now because of the emergence of FinTech applications that provide benefits to consumers by accessing or aggregating this data.

The financial sector and its customers are crossing a frontier and the regulatory framework has not kept pace.

The way in which some of these applications currently work is by using 'screen scraping' technology, allowing 'read only' access, which requires the customer to provide their internet banking usernames and passwords. Other applications require 'read and write' access to perform particular functions, such as sweeping small amounts of money into different accounts.

The current method of access is highly problematic, plagued by regulatory uncertainty, and potentially invalidates a consumer's protection under the e-Payments Code from liability for unauthorised transactions. It raises significant fraud and security concerns for individuals and ADIs.

The e-Payments Code, administered by ASIC, protects consumers against unauthorised fraud and loss on their account if the customer does not disclose their Personal Identification Number (PIN) or password to a third party. If a consumer discloses their PIN to a third party via an app or website, and there is an unauthorised fraud or loss on the account, there is doubt about which party is liable in this scenario. Liability for unauthorised transactions must be borne by either the ADI or the consumer, unless some risk is assumed by the third party.

COBA sees a case for the e-Payments Code to be amended to ensure consumers are protected in this scenario and to allow for some risk-sharing by third parties that benefit from access to customer data.

Notwithstanding the necessary changes to the e-Payments Code, COBA's view is that industry could work together to develop a framework to allow FinTechs, with customer consent, access to customer data held by ADIs. Such a framework would reduce costs to industry, improve and standardise the customer experience and build in sufficient protections to promote confidence in the model.

Open APIs

COBA suggests that one potential solution is the use of open APIs. The term 'Open API' refers to a common language for an application programming interface that would

[6] For an explanation of costs and benefits of CCR, see ARCA's submissions to the ACCC on PRDE.
[7] For further information on the costs of CCR for smaller credit providers, see Veda's second round submission to the ACCC PRDE authorisation process.

provide programmatic access to a proprietary software application. Open, in this context, means that the APIs are standardised so that they can be used across the industry as a way to share data, thereby reducing costs. Open APIs allow customers to authorise the sharing of their account data held by their financial institution with a third party, including FinTechs. Both the United Kingdom and the European Union are moving towards data sharing and open APIs. The PC's Issues Paper identifies the UK's open banking standard as an example of sharing of customers' data by using open APIs.

In May 2016, the UK's Competition and Markets Authority released a provisional decision on remedies indicating that the UK will introduce open APIs. The EU, by adopting the revised Directive on Payment Services, will implement measures that will allow consumers to access and share data about themselves with trusted third parties, including FinTechs.

Greater access to data via open APIs has the potential to promise new and innovative financial services to be developed for consumers. Consumers can be empowered because they will have greater access to information about themselves to better and more accurately compare products from different financial institutions based on their patterns of use.

Customer owned banking institutions have highly competitive pricing and excellent service and are well placed to take advantage of such tools delivered via open APIs. For example, credit cards offered by customer owned banking institutions, compared to the major banks, have substantially lower rates, more interest free days, and lower annual fees[8].

While COBA supports, in principle, open APIs, there are a number of issues that would need to be resolved before open APIs can adopted be in Australia.

One way to resolve these issues is through a co-regulatory approach to develop a framework for open APIs. A voluntary co-regulatory regime could involve legislative reform so that all entities wishing to access ADI account data under an open API regime must meet minimum probity and competence requirements, and comply with a business-to-business code of practice.

Legislation could establish legally-binding minimum requirements which would have to be reflected in the code. Interested industry stakeholders would develop the code consulting widely. Participants in this process might include banking and finance sector industry bodies, such as the Australian Payments Clearing Association, and FinTech bodies.

The code could be signed off by the relevant government regulators (e.g. ACCC for competition, APRA for prudential safety, ASIC for consumer protection, OAIC for privacy).

Industry would then administer the code on a user pays basis, subject to a periodic review process. Only entities willing to operate within this framework would be permitted to access data through open ADIs.

A recent precedent for this is the co-regulatory model developed by industry for comprehensive credit reporting in Australia. A similar approach is being taken in the UK.[9]

COBA is opposed to Government mandating open APIs, which would likely lead to unintended consequences that may ultimately harm consumers.

Below is a list of considerations that would need to be addressed in the development of a co-regulatory model.

[8] Based on data sourced from the Canstar Online Database, 17 June 2016.
[9] https://www.gov.uk/government/news/cma-wants-banks-to-work-harder-for-their-customers

Consumer Protection and Fraud Risks

Banking institutions are trusted custodians of their customers' data and will not support any proposal that does not adequately ensure the protection of customer data. This includes protection against unauthorised access of customer data and breaches of their privacy by third parties.

This is recognised in the Issues Paper, which states that, *'for the economic benefits of data to be fully realised, it will be essential to maintain individuals' and businesses' confidence and trust in how data is collected, stored and used.'*

Trust is an essential pre-requisite for data sharing to be embraced by consumers.

A key component to establish this trust is to ensure that consumers are able to give fully-informed consent before they allow access to their data by a third party. Informed consent means that a consumer understands who they are sharing their data with, for what purpose, and for how long the authorisation will last. Consumers must also have the ability to revoke access for a third party at any time.

Banking institutions are subject to a number of regimes that ensure the protection of their customers' data. Third parties, including FinTechs, must demonstrate their compliance with at least comparable standards. Appropriate security safeguards and protocols will need to be developed so that customers can trust that their data is secure and only used for purposes that they have authorised.

Cost

The issue of costs associated with making data available to third parties has been identified in the Issues Paper, which states that, 'increasing the availability of data is not costless.' However, the paper is silent on who should incur these costs.

As a general principle, banking institutions should be able recover costs involved in establishing capacity to allow third parties to gain access to customer data. There are significant costs in storing, maintaining, organising and providing access to data. There are also substantial costs in implementing open APIs and making customer data available. Costs of developing open APIs should be borne by all parties who benefit.

Data as a source of competitive advantage

Customer data is a source of comparative advantage for banking institutions over their competitors, including new entrants. A balance will have to be found between the right of institutions to protect their competitive position and allowing their customers to provide data to third parties.

One solution would be a voluntary, co-regulatory regime, where banking institutions could choose to participate in an open API scheme. Ultimately, customer demand and a new competitive dynamic will determine the level of participation in the scheme.

Access to Government data sets

The Issues Paper seeks feedback on what high value data sets the Government should share with businesses.

COBA supports allowing highly regulated entities such as ADIs to be able to utilise Government databases to meet their regulatory obligations.

For example, ADIs are required under anti-money laundering and counter-terrorism financing (AML/CTF) laws to verify customer identity. ADIs rely heavily on government issued documents, such as passports and drivers licences, to meet this obligation. ADIs use the Federal Government's Document Verification Service (DVS) for this purpose but the DVS does not verify a customer's address, a key piece of identifying information used by financial institutions to meet their AML/CTF obligations.

AML/CTF obligations place a significant regulatory compliance cost burden on ADIs. Better capacity to use Government databases to confirm data such as a customer's address will assist ADIs to more effectively meet their obligations while reducing their compliance burden. This means lower costs and less friction in opening new accounts and that will promote competition and consumer choice.

COBA looks forward to further engaging with you and your PC colleagues on these matters. Please contact Sally MacKenzie or Alex Thrift to discuss any aspect of this submission.

Yours sincerely

LUKE LAWLER
Head of Public Affairs