Treasury Open Banking Review

Response to Issues Paper
22nd September 2017

1. What data should be shared, and between whom?

In the first instance, major banking institutions will most likely favour a cautious approach in terms of what data should be shared and who should have access to it. This is understandable and makes sense given the need to protect hard-won consumer confidence and digital trust within the Australian Financial Services sector. It is important however to ensure that the deployment and evolution of more sophisticated services is not unduly restricted once initial service offering learnings have been applied.

There is a trade-off between publishing relatively benign data used to prove the system, and more powerful information that Financial Technology (FinTech) companies can exploit, providing business revenues for themselves and high-value services to Australian consumers. Basic transactional data and account balances are currently exchanged by many institutions through pre-existing B2B (Business to Business) arrangements so this is not a new concept for them to contend with. It would be highly beneficial, and increase the opportunity for third party developers to produce niche applications, if PII (Personally Identifiable Information) such as name and address was also shared at an early stage.

The addition of Loan conduct data to the service suite may require more formal accreditation of third party consumers. It might prove invaluable in assisting industry efforts towards mandatory Comprehensive Credit Reporting (CCR), potentially also enabling more sophisticated information to be provided on behalf of consumers wishing to apply for credit, streamlining that process.

Online Lending and Customer Onboarding are current banking practices that would greatly benefit from improved streamlining through automation. If KYC (Know Your Customer) data were shared as part of a formal identity management framework, and with appropriate consent from individuals, lenders could acquire KYC information directly from a trusted identity provider, such as another institution.

Recommendation:

- Adopt a phased approach to exposing customer banking data, initially focussing on simpler, low-risk information to prove the capability as the industry, consumers and FinTech companies learn to effectively interoperate.
- Make a commitment to broaden the volume and types of data made available, with a published roadmap of services to be offered in the 18-24 months following launch.
- Consider KYC data services being made available early on to facilitate a more streamlined digital consumer experience

2. How should data be shared?

Data should be shared using RESTful APIs, exposed in line with agreed standards such as OAUTH 2.0, OpenID Connect & FAPI (Financial API). Each institution should be responsible for providing access to the necessary data and ensuring infrastructure is appropriately architected and scaled to meet the agreed set of standards.

While larger FIs may wish to establish and maintain a direct relationship with third parties such as FinTech companies, the use of an intermediary or aggregator should be

explored as an aid to entry for smaller institutions. This entity could be an existing player in the sector or a new entrant to the market specifically targeting this business. Institutions would connect with the intermediary and deliver data in line with agreed data exchange specifications. Consideration should be given to making this role available to multiple players, encouraging competition and innovation.

Specifications for data formats and sharing of that data should be co-developed with institutions to ensure alignment across all Australian banking systems. If used, the chosen intermediary would act on behalf of each institution, offering a standard set of API services to a potentially unlimited number of third parties. These services would be published and accessible to any qualifying fintech via a public portal. This approach would streamline access to multiple institutional datasets for any fintech developers through a single access point.

Institutions could control which third parties they wished to provide data to, through a control layer established between themselves and the intermediary. Access could be dynamically enabled and disabled without the need to develop bespoke interfaces to each institution.

Recommendation:

- Adopt RESTful APIs and adopt pre-existing, robust security and access management standards such as OAUTH2.0, OpenID Connect and FAPI
- Support a model involving intermediary's or data aggregators to optionally act on behalf of FIs, facilitating connectivity with Fintech companies
- Publish APIs publicly to encourage a technology development community

3. How to ensure shared data is kept secure and privacy is respected?

Given that Open Banking exists globally to provide greater choice for consumers, giving them easier access to, and more control over, data relating to their finances and transactions, customer permission would be required prior to sharing this data with third parties. With implementation of data breach notification legislation now imminent in Australia, FIs will be increasingly concerned with ensuring appropriate controls are in place to determine where responsibility for secure management of this data rests.

As part of providing consent for transference of data, clear terms and conditions relating to the ownership of that data and actions permitted by any recipient parties would need to be agreed. If the use of an intermediary is adopted, this body could act as a broker to hold customer acceptance information independently of institution. This could also assist in account portability between institutions, ultimately removing the direct association of customer data with any given entity.

Potentially, the New Payments Platform (NPP) payID could be used as a proxy for registration and associated approval to release banking data associated with consumer accounts. The NPP is already an emerging platform with pre-existing connectivity to over 50 participating domestic financial institutions.

Recommendation:

- Responsibility for security at all stages of the data lifecycle needs to be clearly defined and published to all affected parties

- Consumers must be provided with a simple, clear explanation of their obligations and what providing consent means to their data
- Consider adopting the NPP payID to assist with consumer registration and Open Banking administration

4. What regulatory framework is needed to give effect to and administer the regime?

The banking industry is prone to large, complex frameworks that can be onerous to administer and which place a significant compliance burden on institutions. Many Australian mutual banking institutions are constrained by resource and would welcome lighter-weight frameworks that recognise and respect variables such as size/scale, complexity and depth and range of customer-product offerings.

It is suggested that a set of guiding principles for a regulatory framework should include the desire to protect the consumer, their data, and the need to ensure the perceived strength of the Australian banking sector is not undermined.

While not absolving FIs of their data security obligations, if the intermediary model were to be adopted, these entities should be subject to regulatory scrutiny given that they have access to significant volumes of sensitive consumer data and may hold or buffer quantities of this data for purposes of operational efficiency.

A further role is potentially valid in this model, that of a third party registrar. The registrar would undertake the necessary due diligence, legal review, privacy and insurance compliance activities on the third party consumers of customer data. This would present significant administrative efficiencies for the sector. Different levels of compliance may be recognised with resultant varying access to customer data. For example, a new FinTech start-up business might achieve compliance with requirements for accessing transactional data but not loan conduct data. This would be captured by the registrar and the intermediary would restrict transference of data between this business and any third party consuming service.

Connecting all intermediaries with the registrar would provide an opportunity to fast-track "switching on" new FinTech businesses as soon as they were viewed as compliant, rapidly facilitating access to a comprehensive set of industry data. Ideally, the accreditation or status of participants should be made public to provide transparency of risk when consumers sign up and provide consent to third party services.

Recommendation:

- Endeavour to implement a lightweight regulatory framework that protects the consumer but is not overly onerous to comply with for smaller FIs and third-party consumers
- Consider the role of Registrar to centralise administration, especially initial and ongoing third party compliance assessments to agreed standards

5. Implementation – timelines, roadmap, costs

While Open Banking has the potential to be a significant undertaking for the industry, it could be explored in a pilot or proof-of-concept mode with a smaller selection of institutions. Timeframes for this could be 12-18 months with learnings using to inform a more widespread deployment with a refined and more robust management

framework. Finding the necessary FinTech businesses willing and able to participate should not be a problem given their ongoing requests for precisely this information.

The suggestion in the Coleman Report that banks provide open access to customer and small business data by July 2018 seems a little ambitious to achieve at scale. Rather than adopt a big-bang approach, it might be beneficial to prioritise transactional and account data initially, certainly if this was to be mandated. Credit reporting and then KYC and identity information might then follow. This ordering reflects a combination of demand and implementation complexity and risk.

Costs could vary significantly depending on whether institutions wait or implement Open Banking independently, ahead of any mandated federal regime. The latter option still presents many unknowns that make estimation of costs difficult.

A solution which provides flexibility for the providing institution would involve the implementation of a number of components such as an identity and access management framework, an integration platform and a set of appropriate APIs into the core banking system or data warehouse. Many of these components may already exist or be planned within medium-sized or larger institutions. Resourcing to develop, configure and manage ongoing maintenance of these components will also be necessary, along with third party consulting and specialist service delivery management costs.

For institutions that have not yet made these types of technology investments, this could present a significant barrier to entry. However, even with the need for material investment, the repurposing of the technology is certainly possible so sunk costs could yield ongoing additional value within each institution, independently of this initiative.

Broad indications are that technology costs could be in the region of $250K per annum to implement and manage an Open Banking solution for an institution that is perhaps $1-5 billion in asset size. Ongoing costs may be slightly lower once the open banking regime is bedded down although much of it will be associated with recurring subscription charges for infrastructure and platform licencing. An additional up-front investment, perhaps in the region of $75K would be required to research and implement necessary internal processes, procedures, compliance and other legislative obligations. These might then likely incur ongoing operational costs in the region of $25K pa.

Recommendation:

- Consider a small-scale pilot or trial with a restricted number of FIs to prove theoretical concepts and gain traction with FinTech companies and progressive institutions
- Prioritise transactional and account data initially

6. Additional Considerations

There is potential for this to be a revenue-generating service for the providing institutions. Fees could be charged to third parties or intermediary's based on the number of connections, volumes of data and types of data. It is conceivable that revenue could exceed support and maintenance costs for running these platforms. It is likely that the intermediary would charge third party consumers for access to the

underlying data and at least part of this revenue should be passed back to the providers.

Consideration given to such things as speed of access to data, latency within the system, timeliness of data (overnight batch or dynamic) and costs of achieving these requirements to ensure that smaller institutions are able to use the service.

A low-cost option for small FIs unable to make the necessary capital investment to self-manage this capability might be to permit an intermediary to securely and directly access a subset of that FI's customer data, then serve that content to approved third parties through published APIs. Only data for those customers that have provided consent would be available for consumption.

FinTech businesses are typical small, nimble and resource poor and often suffer cash-flow challenges. They differ significantly from most FIs and accelerating the registration and due diligence process through a managed intermediary would significantly aid in building a broad, competitive technology community that can take advantage of Open Banking and deliver tangible value to Australian consumers.

Institutions could potentially approach Open Banking in different ways, however it is likely that the associated services will be offered to consumers in a similar manner to other financial products. Therefore it is suggested there would be additional costs associated with Marketing, Technology, Operations and Sales as well as ongoing involvement with Risk, Governance, Compliance and Internal Audit teams. Centralising the promotion of Open Banking with shared collateral would be advantageous and provide a more cohesive and compelling proposition for Australian consumers.

Recommendation:

- Encourage institutions to consider the revenue-generation aspects of this service rather than simply view it as surrendering control of data
- Ensure appropriate platform performance requirements are defined and published
- Consider alternate data interchange options for smaller institutions that cannot justify capital investment but wish to offer contemporary services to their customers
- Consider development of centralised information resources that can be reused by all platform users for consistency of messaging

Head Office
Technology Park, Madgwick Drive, Armidale NSW 2350
PO Box U631, University of New England NSW 2351
Telephone 132 067 **Email** enquiries@regionalaustraliabank.com.au
Web regionalaustraliabank.com.au