SUBMISSION PAPER:

Submission to Open Banking Inquiry

SEPTEMBER 2017

This Submission Paper was prepared by FinTech Australia working with and on behalf of its Members; over 170 FinTech Startups, VCs, Accelerators and Incubators across Australia.

Table of Contents

About this Submission

This document was created by FinTech Australia in consultation with its Open Data Working Group, which consists of over 120 company representatives. In particular, the submission has been compiled with the support of our three Working Group Co-leads:

- Luke Howes, Proviso (https://proviso.com.au/)
- Peter Lalor, Money Brilliant (https://www.moneybrilliant.com.au)
- Tommy Mermelshtayn, ZipMoney/Pocketbook (https://zipmoney.com.au/ & https://getpocketbook.com)

This Submission has also been endorsed by the following FinTech Australia members:

- Luke Howes, Proviso (https://proviso.com.au/)
- Peter Lalor, MoneyBrilliant (https://www.moneybrilliant.com.au)
- Tommy Mermelshtayn and Bosco Tan, ZipMoney/Pocketbook (https://zipmoney.com.au/ & https://getpocketbook.com)
- Damir Cuca, Basiq (https://basiq.io)
- Greg Einfeld, Plenty Wealth (https://www.plenty.com.au)
- Joanne Cooper, ID Exchange (https://idexchange.me)
- Mike Page, Meeco (http://www.meeco.me)
- Peter Colbert (https://www.inamo.com/)
- Boyd Pederson, Bigstone (https://www.bigstone.com.au)
- Beau Bertoli, Prospa (https://www.prospa.com/)
- Sam Brown, Pelikin (https://pelikin.co/)
- Stuart Stoyan, MoneyPlace (https://moneyplace.com.au)
- Stuart Grover, Look Who's Charging (https://lookwhoscharging.com)
- Jacqueline Park, Carrots Money (https://www.carrots.money)
- Alan Yeo, MoneyMe (https://www.moneyme.com.au)
- Lachlan Heussler, Spotcap (https://www.spotcap.com.au)
- Daniel Alexiuc, Living Room of Satoshi (https://www.livingroomofsatoshi.com)
- Danny John, SocietyOne (http://www.societyone.com.au)
- Julian Hedt, Banjo (https://www.banjoloans.com)
- Jonathan Shaw, Moneysoft (http://www.moneysoft.com.au)
- Leon-Gerard Vandenberg, Rights Commerce Ltd (http://rightscommerce.com)
- Ben Ford, Yodlee (http://yodlee.com)

Submission Process

In developing this submission, our Open Data Working Group held a series of Member roundtables to discuss key issues relating to and in addition to those raised in the Issues Paper:

- Current financial market microstructure
- Developments in overseas markets
- Regime Applicability
- Scope of Data included

- Data Security
- Privacy
- Liability
- Accreditation
- Pricing
- Timeframe
- Technology (or, Technology agnosticism)

We also particularly acknowledge the support and contribution of Baker McKenzie, K&L Gates and King & Wood Mallesons to the topics explored in this submission.

Glossary of Terminology used in this submission

Throughout this submission, FinTech Australia uses certain terms to describe different facets of the issue. A few of the more important ones are specifically defined to aid comprehension:

Application Programming Interface (API) - An API is a set of commands, functions, protocols, and objects that programmers can use to create software or interact with an external system. It provides developers with standard commands for performing common operations so they do not have to write the code from scratch.

Consumer / Customer - In the context of this submission, the use of the word "consumer" refers to both individual consumers and small businesses. It may also be used interchangeably with "customer" when referring specifically to a set of consumers who may be customers of an institution.

Open Data - Open Data is the common phrase given to movements, both politically and technically, to create a policy framework or context that allows freer access to and movement of data from one party or group of parties to another or others. It may reference data owned or held by either individual consumers, small or large institutions, or governments.

Open Banking / Open Bank Data - Open Banking is used in this submission to describe the current inquiry, which is focused on creating a viable, safe and secure Open Data framework for Bank-held data. Given the specific use of the word "Bank", it is assumed to mean Bank product information, as well as current transaction account data relating to a bank's customers.

Open Financial Data - This phrase is used in this submission to refer to the holistic application of Open Data frameworks to the entire financial services sector, including superannuation, insurance and other financial products as well as Banks. It is FinTech Australia's view that this is ultimately the goal of Open Banking.

Executive Summary

An Open Financial Data regime is key to giving consumers greater access to and power over their data, empowering them with more choice, greater understanding of their financial standing and more control over their financial futures. It is also vital to supporting greater fintech innovation - which creates increased competition, greater choice, more efficient delivery and lower price of financial services for consumers.

A bold, clear, mandated timing is critical - many other leading financial services jurisdictions are already underway with various Open Data policies. Financial Services Institutions (FSIs) and Bank competitors across the region are already rapidly embracing Open APIs to meet regulation in their own jurisdictions' regimes. If there is no mandated timeline, there is no incentive for Australia's traditional financial services players (and fintechs) to implement. They will ultimately be left behind other global competitors that may move into this market, having integrated better fintech solutions for their customers faster than our local players. It will create a substantial risk to Australia's current position as a leading regional market for fintech innovation and investment.

We must move quickly to establish a series of use-case oriented working groups comprised of Industry (large and small), Government and Consumer groups to develop and determine how minimum security standards, privacy and liability will be treated for each use case. This standards development must be also done to bold, clear timelines.

Much can already be drawn from work in the UK, and also the EU's PSD2 and GDPR regimes which are appropriate models for Australia, with the exception of the ruling to eliminate screen scraping. The EU model in particular is relevant to Australia, as it applies to all institutions equally, and APIs allow consumers to direct third parties to initiate ("write") decisions as well as to share data ("read") to compare products/services. The desired policy outcome of improving competition and making it easier for consumers to switch to more appropriate service providers is only possible if APIs also enable consumers to direct an institution to act to deliver an outcome, as well as to share data for comparison.

Data aggregators that act with a consumer's permission to retrieve their bank data (often known as 'screen scraping') should also be formally legitimised by recognising them within ASIC's ePayments code (subject to them being accredited as meeting certain minimum security standards) - unlike other jurisdictions, Australia's fintech industry is heavily reliant on scraping. Stopping data aggregators who utilise scraping techniques would kill the current fintech industry. It also provides a lower cost alternative for smaller banks, fintechs and institutions to innovate faster and meet their compliance obligations under any new regime, and means they may move to full API integration within a timeframe that suits them.

Introduction: Open Banking in Australia

FinTech Australia has been a consistent advocate for policy reform to drive the implementation of an Open Financial Data framework in Australia before the end of 2018.

From our very first policy reform recommendation paper to Federal Treasury in February 2016, which saw the launch of the Federal Treasurer's *Backing Australian Fintech* initiative, and through our two submissions to the Productivity Commission's subsequent inquiry into *Data Availability and Use*, we have continuously advocated that the government mandate the development and implementation of a standardised "Open Banking" model to put customers in control of their data, empowering them to share their data with third parties of their choice in order to understand their financial situation, and make financial decisions that are best for them.

Data isn't just valuable for individual consumers – it is incredibly valuable for small businesses as well. Many of our member companies enable small businesses to access their financial data, and to build a robust financial picture within their financial management software. There are tremendous economic gains that may be realised by giving small businesses greater power to use their data with third parties to obtain better-priced financial products and services. As such, as we mention "consumers" throughout this document, please note that we are also referring to "small businesses."

FinTech Australia's members believe an Open Financial Data regime will do the following (and indeed this view is also reflected in the Terms of Reference for this inquiry):

- Improve choice, improve access to, and increase competition in financial services, in order to drive better financial outcomes and experiences for Australian customers and businesses;
- Improve the efficiency of the Australian economy by reducing manual transfer and analysis of data;
- Expedite the development and testing of new financial innovations in Australia; and
- Ensure the Australian financial services industry remains competitive with businesses, both traditional and new/emerging, from other global jurisdictions.

Australia's is currently considering implementation of an Open Banking framework similar to what is being advanced very rapidly in other world-leading financial centres such as the United Kingdom and the European Union (see section on International context below).

However, despite the lack of a formal policy framework for Open Financial Data in Australia and the historical reluctance of Australian financial institutions to make customer financial data available, there is already a vibrant Australian fintech ecosystem based on permissioned access

to consumer data, provided by a community of data aggregators and accounting software providers.

Some of these aggregators rely on the fintech company's customers providing their online banking credentials (typically their online account number and password), allowing the data aggregator to log in to their online banking portal, and to collect and format their transaction history data on the customer's behalf. This process is sometimes known as 'screen scraping', and is the means by which the majority of fintech companies - consumer-facing fintechs in particular - obtain the customer data required to power their offerings.

As a result of technological advances and market developments, fintech companies are now utilising data from a number of different sources, providing products that allow customers to:

- Forecast 'safe spending amounts' over a coming period, based on their historical behaviour of bill payments and other expected outgoings, along with understanding in which categories they are spending the most money;
- More easily apply for, and in some cases obtain cheaper credit, as the lender is able to get a fine-grain record of recent transactions and make a more accurate determination of their risk profile. It would also allow lenders to meet and exceed their responsible lending requirements as they will be able to see future customer commitments, and their capacity to repay their loan;
- Pre-fill tax return deductions, resulting in considerable time saving for both consumers and businesses;
- Invest small change left over from online purchases into bank accounts and into superannuation, as a convenient form of goal saving or wealth generation;
- Get a holistic view of their personal, business', or family's financial standing, by integrating multiple financial products, potentially from numerous product providers and data sources, into a single interface or dashboard; and
- Prove their identity to others when applying for a financial product or service, via a more convenient online means.

Fintech companies, sophisticated data aggregators and exchanges are also providing products that allow small businesses and institutions to generate positive economic outcomes by:

- Facilitating access to data from other ecosystem partners through direct agreements with financial institutions; and
- Facilitating access to insights created through the secure exchange and analysis of de-identified data from multiple institutions.

There are shortcomings however in the current approach to customer data collection and reuse, however, as outlined below:

- FinTech Australia members report that anywhere between 10-50 per cent of potential customers baulk at handing over their passcode, irrespective of strong security and

privacy measures. This significant barrier on customer uptake is discouraging innovation in this area.

- Some in the fintech community believe that there may be faster technological solutions available, compared to screen scraping.
- There have been concerns that banks have been advising customers against giving their passcodes as a means of stifling competition - as was cited by one member in a submission to the Coleman review. [1]
- The existing ePayments Code - prepared by the Australian Securities and Investments Commission (ASIC) - does not adequately address customer rights and protections in this new open data environment. The Code is also currently only a voluntary code, and is not endorsed by all relevant financial institutions.
- For permissioned parties, including data aggregators and consumer-facing applications, some of the most significant obstacles are disruptions in the flow of data (particularly when there are changes made to bank IT processes), data that are unreliable, and high latency in the receipt of data from the account provider. For consumers, these same obstacles can cause more harm than simply confusion and inconvenience.
- The breadth and depth of data available across Financial Services Institutions (FSIs) is inconsistent, making it hard to efficiently provide comparable services between institutions.
- There is no uniform view amongst FSIs on repercussions, should customers engage with these innovative solutions and their accounts are subsequently compromised.
- Use of these aggregator services can also present commercial challenges to start-ups.

In saying this, many fintech companies are happy with existing screen scraping solutions, and are likely to continue to use these solutions even when alternative technology is available. At present, screen scraping creates a strong platform for innovation in Australia, and measures should be taken to ensure that its current application in fintech innovation is not disrupted as the market evolves to make other technology approaches available.

Many Australian FSIs have now come to accept that Open Banking is inevitable, and have made submissions and statements concerning a multi-billion dollar cost of implementation - an amount proven to be inflated compared to similar investments made by international banks, provided in our prior submissions. Several FSIs have also claimed that the development of the required security and privacy standards will require a lengthy (2 year plus) and detailed stakeholder consultation process in order to safeguard consumer interests.

Despite these statements, tremendous progress has already been made by other FSIs globally, who are operating in jurisdictions well underway in the implementation of their own Open Data regimes.

[1] https://www.ifa.com.au/news/17668-cba-refutes-acorns-competition-allegations

Indeed, many global banks, including Clydesdale Bank[2], Citi and even more recently Macquarie Bank in Australia have proactively launched Open Banking APIs[3] - not in order to comply, but rather to decrease the cost, and increase the speed of testing new innovative fintech solutions that might provide a competitive advantage and better customer experience than their rivals.

Some departments within the big four banks have also recognised that open data is coming, and have already started taking steps toward implementation - an example is NAB Labs who have already begun making some Product information available via Open APIs in hackathons, and Westpac with their launch of Data Bank.

The provision of products and services through digital means has meant that the most successful companies have been the ones best able to access, analyse and utilise data. The same is increasingly true in financial services; large digital players such as WeChat (WeBank and WePay), Ant Financial (AliPay), Google (Android Pay), Apple and even WhatsApp[4] have begun testing banking and payment services in markets such as China, India and even here in Australia. The substantial reach (via their existing communication channels) and vast amounts of capital available to these digital players makes it easy for them to obtain alternative sources of data, and invest in resources to source, test and deploy innovative new solutions to millions of customers at a very low relative cost.

Without access to the financial data necessary to build, test and deploy innovative fintech solutions in their local market, Australian companies stand little chance of being able to compete on an increasingly global stage against these digital juggernauts. The net outcome of this is that increasing amounts of our tax revenue, and best skilled labour will go offshore.

Likewise, it is also crucial to ensure that the legislation is designed to be balanced, requiring compliance from all financial data-handling institutions - including the large global digital players. If not, we risk handing an unfair advantage to these international players at the expense of both local fintech companies and large FSIs alike.

[2] Eyers, J - *Clydesdale says Open Banking will help it compete*, Australian Financial Review, May 2017
[3] Eyers, J - *Macquarie trumps big four with new Open Banking Platform*, The Australian Financial Review, September 2017.
[4] Sukumar, A - *WhatsApp's Integration of UPI-Based Payments Has Strategic Consequences for India's Digital Economy,* The Wire India, August 2017.

International context: Open Data around the world

Below is an updated overview of other jurisdictions that are in the process of implementing Open Data policy that is relevant to financial services, and the scope and implications of each.

Comparison Table	
Jurisdiction	**Latest Update on Open Data policy**
United Kingdom	In late 2016, after a review that found that the largest UK banks do not have to work hard enough to acquire and retain customers, the UK Competition and Markets Authority (CMA) mandated the 9 major bank institutions to fund the creation of an Implementation Entity, which would be responsible for overseeing the development of standards for, and deployment of Open Banking APIs by these 9 major banks, with read and write capability by January 2018. Whilst the first milestone of releasing 'Open Data APIs' for non-customer related data such as ATM locations and product comparison information was met in March 2017, at this point in time it is not clear whether the second major milestone of deploying full read/write APIs for customer transaction data will be delivered by January 2018. However, specifications for these read/write APIs have been released by the UK Implementation Entity since July 2017.
European Union	PSD2 which aims for enactment by member states in January 2018, and has a greater scope for movement of consumer information than does the UK's Open Banking (more extensive types of account are covered) and GDPR (the EU's May 2018 data protection measures) also impacts consumer rights over data. Individual jurisdictions within the European Union are noted as advanced in the open banking arena, Germany is seen as one of the most open banking environments in the world.
Japan	Amendments to the Banking Act forcing Banks and Credit Unions to create open APIs was passed in May 2017, and is expected to come into force around March 2018. The law is intended to encourage greater collaboration between banks and fintech companies. The Japan Financial Services Authority also introduced a registration system for companies connecting to these APIs.
India	Since 2009, the Indian government has been building a centralised Unique Digital Identity system known as Aadhaar, with a target to have all 1.28 billion Indians citizens registered on the system by March 2017.[5] The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 was passed as a money bill on March 16, 2016, making it mandatory for a person to authenticate her/his identity using the Aadhaar number before receiving any government subsidies, benefits or services - an initiative that is estimated to have created over US$400m in cost efficiencies for the government in benefits distribution[6]. Increasingly, large institutions such as Banks and Mobile companies are also making it mandatory for consumers to provide their Aadhaar ID to fulfil their eKYC compliance requirements due to the reduced cost and

[5] https://thefinanser.com/2016/09/indias-billion-people-digital-identities.html/
[6] http://www.aadhaarnews.com/multiple-facts-aadhaar/

	improved efficiency of using it. There has, however, been a small amount of consumer backlash relating to Aadhaar and its intersection with India's fundamental right to privacy[7], which is now in front of the Supreme court. The Aadhaar Act also introduced the launch of a Universal Payments Interface (UPI) leveraging Aadhaar, in recognition of innovative mobile payments fintech companies such as PayTM that were helping to digitise much of India's banking and commerce. Since its deployment, many major international digital companies such as WhatsApp and Google have used the new UPI API to test new payments products in this market.
US	There has not been a legislative intervention in the United States; data aggregators have sought arrangements with major banks on a one-to-one basis. Innovate first, govern second has been the US approach. Scraping via the provision of username/password to third parties is still a major means of obtaining customer data with a range of inherent risks. The current Federal government is unlikely to intervene. Industry is having to self-regulate, which is sometimes of concern to consumers when high profile problems arise. JP Morgan Chase has made a high profile agreement with personal financial app provider Mint (owned by Intuit and therefore providing a higher level of confidence to a large bank) in the last few months. A further example is the Wells Fargo agreement with Finicity. The McKinsey article on Open Banking provides a helpful overview.
Singapore	The very specific business and political context of Singapore, particularly the strong guidance and leadership from its regulator, the Monetary Authority of Singapore (MAS) has led to high Bank co-operation in order to produce data exchange systems, particularly around eKYC. This has now expanded to the extent that there is less need even for consumer credit bureaux.

[7] https://thewire.in/176528/former-ag-mukul-rohatgi-india-right-to-privacy/

Why an Open Financial Data regime is great for consumers

As mentioned in the Introduction, fintech companies are already providing significant customer benefits as a result of being able to access customer data, with the potential for even greater benefits under a formal framework. Below are a number of case studies from companies currently using data to deliver consumer benefits in Australia.

Pocketbook is a Sydney-based company which first launched in its budgeting tool to the market in October 2012.

Pocketbook allows users to easily see the categories in which they are spending the most money. The tool links to your accounts and automatically allocates most of your spending to set categories - such as groceries or utility costs - however also allows you to set up new categories. By tracking regular expenditure (including upcoming bills) and income, the tool also gives advice to users on how much they can 'safely spend' in coming days or weeks.

During tax season, Pocketbook also has an web feature which helps customers automatically detect deductions for tax time – a previously tedious manual and paper-based process.

All the above helps people get faster and clearer insights into where their money is going and therefore an opportunity to regulate their behaviour to save money. It also helps people spend money at the right time and therefore not be caught short.

Another Sydney based fintech business, **MoneyBrilliant**, is using customer financial data, acquired by permission from customers through a data aggregator, combined with non financial data about household bills to find cheaper deals for the customer.

The business recently launched this service to help customers find the cheapest deals on gas and electricity bills and plans to extend the service to cover other household bills and expenses in the near future.

MoneyBrilliant also combines the customer's data with data available from the Australian Bureau of Statistics and the Australian Taxation Office to help customers compare their spending and income to people like them based on where they live, their occupation, how much they earn and their net worth.

Examples such as this clearly demonstrate the potential to deliver enormous consumer benefit both from the implementation of an Open banking regime and from extending the regime to other sectors of the economy.

Another example is **Spotcap**, which was launched in Germany now operates in countries around the world, including Australia. It opened its Sydney office in May 2015.

Spotcap, and other small business fintech lenders like it, are filling a major market void left by banks and other traditional financial institutions.

Spotcap has developed its own software to access and analyse the relevant financial data of prospective clients, including through 'screen scraping' this data with client permission.

This allows Spotcap to make a quick (generally less than 24 hours) decision on finance applications. It also allows Spotcap have an increased level of confidence when providing finance and therefore the ability to quote highly competitive rates.

As at July 2017, Spotcap had extended more than $52 million in credit to small businesses, after analysing more than seven million lines of credit bank data. This illustrates the huge potential of data access in creating great financial services outcomes for Australian businesses.

Potential future consumer benefit scenarios

Interviews with FinTech Australia members have identified a plethora of potential future consumer benefit scenarios, under an optimal and fintech-friendly Open Financial Data framework. These scenarios illustrate why Australia should move to implement this framework as soon as possible.

CONSUMER USE CASES	
Potential use case	**Potential use case description**
Portfolio account switching	You will be able to seamlessly switch all your savings and credit accounts from one institution to another institution, to take advantage of better whole-of-portfolio deals
Portfolio virtual assistant	You can receive advice about your accounts from a friendly 'robo' assistant in written or verbal form and instruct the assistant to make changes to your account following this advice, while you are having breakfast or travelling to work
Automatically pay credit card debts	You can instruct automatic payments of your credit card within certain set parameters, such as if you have sufficient savings at the right time of the month - avoiding hefty interest payments
Automatic interest rate switching	You will receive advice about improved interest rates available for one or more of your accounts, and then instruct the automatic switching of your account to take advantage of this rate

Customer data harvesting	You will be able to make your data securely available on the open market so you can receive significant discounts across all aspects of financial services and other selected areas, as these discounts become available
BUSINESS USE CASES	
Potential use case	**Potential use case description**
Business accounting software downloads	You will find it easier to prepare annual financial reports, because your accounting software can easily access all your account information
Improved access to loans	You will find it easier to access loans, because you've given a lender permission to access your tax payment information which shows strong growth and provides a more contemporary record than your annual financial accounts

Implementation of Australia's Open Banking regime

FinTech Australia welcomes the opportunity to put forward its position on behalf of members in relation to Australia's coming Open Banking regime.

We have done so via a selection of key issues we believe will be important, particularly with respect to ensuring that the desired outcomes - that is, improved choice, greater competition and a better deal for consumers - are met, in a manner that is equally considerate of consumer privacy and security concerns.

Whilst we acknowledge that fintech companies stand to gain substantially from an Open Financial Data regime - we also equally acknowledge the responsibility that comes from being entrusted with a consumer's confidence and trust, particularly when it comes to something as valuable as their personal data. Fintechs also aim to grow into larger, successful businesses who will contribute data back into the ecosystem under the Open Financial Data regime, promoting a continued level of innovation as well as vibrant competition.

Furthermore, FSIs that embrace the potential and change will be able to drive competitive advantages and new commercial opportunities; many FSIs are not only providers of account-level information to third parties, but are also beneficiaries of it, and rely on services provided by data aggregators and technology companies to offer their customers financial management tools within their own bank-offered online or mobile interfaces.

Regime Applicability and Timing

Who should Open Banking apply to?

FinTech Australia's members agree that consumers should be empowered to provide permissioned access of their financial data to third parties securely and easily, using whatever secure, accredited application or technology they wish, without undue charges or restrictions that might unreasonably favour any one application or technology over another.

They should also be empowered to act upon the decision that may result from their data sharing; that is, they should also be able to direct institutions to initiate or complete a transaction, or switch their product holding to another institution easily and efficiently if they so choose.

We also agree that this comprehensive right for consumers should equally apply to fintech companies and data aggregators, as well as Banks (i.e. all Authorised Deposit-taking institutions with consumer or SME-facing applications in Australia) and other FSIs that are important for the delivery of sound, holistic financial advice.

In keeping with FinTech Australia's broader fintech policy objective of creating a balanced regime that does not prove onerous for smaller organisations in their establishment phase, we propose a broad compliance threshold for organisations with a turnover of less than $3m, the same threshold specified by the Australian Privacy Principles in the Privacy Act.

However, the exception for this is any organisation that wishes to itself be able to request and obtain customer-permissioned data from another institution, as outlined in the accreditation section below. This would include all Data Aggregators, and the majority of fintech companies.

Phasing and timing of Open Banking roll-out

Consistent with the intent of Recommendation 4 in the Coleman Report, we believe all financial institutions in scope for roll-out of Australia's new Open Data regime within the financial sector should be required to complete their implementation of Open Financial Data measures by the end of June 2019. That is, they must create the ability for consumers to share data (i.e. similar to a "read-only" API), ***as well as to direct an institution to act to initiate a transaction or other desired outcome*** (i.e. similar to a "read/write" API). This should be undertaken as a first, tangible separate step toward the implementation of the broader Comprehensive Right for Consumers recommended by the Productivity Commission.

This may seem like a bold timeline, but it is one that will ensure Australia's financial institutions invest in the technology and capability required to compete adequately with their international peers, given the timing of other regimes discussed previously. Much of the work from other jurisdictions is readily available, so Australia can use this work to save time - but using standards from other jurisdictions will also ensure that greater interoperability is baked in for Australian companies wishing to build global businesses, which is extremely important.

Key to institutions meeting this progressive timeline is the question of whether a specific technology is prescribed, and how the regime is enforced. For example, a policy directive could assert that institutions '*must have a facility by which a consumer may provide permissioned access of their financial data to third parties, by the end of June 2019, and that this facility should be provided to 3rd parties via an API or similar technology to an agreed minimum privacy, security, and service standard*'.

Should this be the case, then it should be possible for all major institutions to comply within a condensed timeframe, given compliance with the regime could either be built by the institution, or by another third party on behalf of an institution, such as one of the many data exchanges and aggregators that operate in Australia. This is explored in further detail under the Technology section below.

FinTech Australia also appreciates that using today's technology processes, it is difficult to enforce a transformative undertaking without providing a clear customer objective, scope, and

rationale. We therefore recommend that Australia's Open Financial Data regime be implemented through a series of roughly 6 monthly phases, with each phase centred on the application and delivery of the regime to fulfil a specific customer or industry "use case". The following table outlines our suggested use cases, which have been selected as priority for both having the widest industry application and greatest consumer benefit, along with proposed timeline and rationale for the selection of each use case:

Phase / timing	**Use case**	**Rationale**
Phase 0: immediate	Establish standards working groups, agree ASIC accreditation process, and legitimise scraping by accredited entities in ASIC ePayments code. Make ePayments code mandatory. Mandate Comprehensive Credit Reporting given target of 40% contribution is unlikely to be met by December 2017.	An ASIC accreditation process will ensure only valid Data Aggregators can continue to access data through the regime, ensuring both consumer data and interests are protected. It will also improve Consumer trust of legitimate aggregators, and prohibit institutions from invalidating their customer protections for legitimate data sharing activities. Legitimising scraping by accredited entities will also allow the industry to continue to operate with confidence. As outlined in the Federal Budget earlier this year, legislation should also be tabled and passed to mandate comprehensive credit reporting, given current projections clearly show that the 40% contribution target will not be met given contributions are still currently less than 30%.
Phase 1: by end March 2018	Allow customers to share their data from public and/or private data sources to easily complete their know-your-customer (KYC) validation for financial products and services. (aka "KYC Reliance")	Starting with a use case that provides common benefit will help establish working cadence and cooperation. It will also help stakeholders get a more complete picture of where important customer information is held, and by whom. Government departments such as the DTA and AUSTRAC are already attempting to align in a bid to create standard frameworks to support multiple providers for a customer's Digital Identity. However, this needs to be done with Industry engagement, particularly as relates to both consumer consent frameworks and KYC. All parties - including consumers, banks and fintechs alike will save time and cost by being able to access and utilise a sanctioned Digital ID for KYC validation.
Phase 2: by end June 2018	Allow consumers to easily share data to compare Current Personal/Business transaction accounts and SME Credit products. (In line with recommendations from the Coleman Review - Parliamentary Inquiry into	This use case fulfils the first policy objective of providing consumers a means to easily compare certain financial products to understand if there may be an alternative that better suits their needs. The scope of data required for this use case will also match that which is currently supplied by Data Aggregators; i.e. current account transaction data. It will provide also similar

	four major banks)	functionality to what aggregators can provide today, i.e. the ability to share customer data via read-only APIs, but will not give the consumer an immediate ability to initiate transactions. In terms of product data which is already largely available from banking websites, data should include interest rates, product type, product maturity date, whether it is fixed vs variable, whether it is interest only or principal and interest, as well as offset account details. The use case also focuses on greater availability of data to encourage broader small business uptake of SME lending, which is of particular importance given perceived lack of competition in this sector by both Federal Treasury and more recently, APRA[8]. It would also make it easier for lenders to proactively apply responsible lending practices.
Phase 3: by end December 2018	Allow consumers to have a holistic view of their financial situation, including their insurances and investments held	This use case also fulfils an important broader policy objective for the financial services sector; that is, to enable consumers to better understand both their short and long-term financial health. Important data is currently held by insurance and superannuation funds concerning consumers' long-term financial well-being, and is very difficult to access. Consumers are currently apathetic to their situation, resulting in inadequate retirement savings which causes stress on Australia's pension system. This phase would bring both superannuation and insurance firms under the new regime, and see the regime expand to include other important product data from Banks such as deposits, loans, investments and other insurance products. This should include not only insurers (life, general, health), and APRA regulated superannuation funds, but also all retail managed funds, stockbrokers and share registries in respect of securities listed on the ASX. By empowering consumers to easily access and share this information, they not only have a means to understand their financial situation, they (and their advisors) can also work out the best course of action to improve it.
Phase 4: by end June 2019	Empower consumers to effortlessly instruct institutions to initiate or complete a transaction, or switch between financial product or service providers on their behalf	This use case will finally realise the full policy intent and benefits of providing consumers with increased choice and competition. The ability to compare between products is only part of a customer's acquisition or switching journey; the remainder is being able to then easily act upon their choice. The implementation of full "read and write" APIs, or API-like functionality, will be critical to allowing consumers

[8] APRA Submission to Productivity Commission Inquiry into competition in Australia's financial sector, September 2017

		to port across their important data and business to a financial service or product provider that suits them best.

To reinforce the point - FinTech Australia's members are strongly of the view that Superannuation, Investment and Insurance firms should also be included as early as possible within the roll-out of Australia's Open *Financial Data* regime - particularly as these firms are critical holders of data that relates to allowing consumers to have an accurate understanding of their financial health, and ways in which to improve it.

Changes to ASIC ePayments Code

The wording of the ASIC ePayments Code is currently a major inhibitor for customer take-up of new innovative open data products. This is because the code indicates that customers may be liable for monetary losses from their account if they hand over their passcode to any external parties. [9] As a result, the evidence is that many customers baulk at handing over their passcode - potentially up to one in two customers.

Despite the legal ambiguity, hundreds of thousands of Australians have shown they are comfortable with handing over their passcode so they can access innovative new financial services. This approach underpins much of the fintech revolution underway in Australia and importantly, has not led to any known security breaches.

While neither the Productivity Commission or Coleman reviews touched specifically on the ePayments Code issue, ASIC indicated it was willing to change the ePayments Code to formally legitimise data aggregation in its August 2016 submission to the Productivity Commission, stating "there is uncertainty amongst consumers and industry about how liability provisions of the ePayments Code relating to account aggregators are to be interpreted. While ASIC has not yet formed a view about how the uncertainty regarding liability can or should be resolved, provided security concerns can be addressed, consumers should not be disadvantaged by their use of legitimate account aggregation services." [10]

The ePayments Code issue was also previously examined by the Australian Government's Financial System inquiry, released in 2014. The inquiry report argued that the ePayments Code should be turned from a voluntary to statutory document, to provide improved consumer protections. [11] The government's response released in 2015 agreed to "mandate baseline consumer protections in the ePayments Code, subject to the code being fit for purpose and technologically neutral." However, nothing appears to have happened since. [12]

[9] See Clause 12 of the ePayments Code at http://download.asic.gov.au/media/3798542/epayments-code-published-29-march-2016.pdf
[10] See page 3 at http://www.pc.gov.au/__data/assets/pdf_file/0006/206439/sub195-data-access.pdf
[11] See page 167 of the http://fsi.gov.au/files/2014/12/FSI_Final_Report_Consolidated20141210.pdf
[12] See https://treasury.gov.au/publication/government-response-to-the-financial-system-inquiry/

It is for these reasons that FinTech Australia recommends that the first initiative, or phase 0 of Australia's Open Financial Data regime, should be to update and mandate the ePayments Code so that it explicitly supports current screen scraping practices. This change to the code needs to happen at the same time that it shifts from a voluntary to a mandatory standard. If it remains a voluntary standard, FSIs may look to opt-out of any amended standard which would cause uncertainty and concern for consumers in the process.

In summary, the ePayments Code should be legitimised by:

- Mandating it as part of the Australian Securities and Investment Commission (ASIC) Act, in line with the 2014 recommendation of the Financial System Inquiry
- Changing the code to make it clear that customers are not liable for monetary losses, where they supply their passcode to a company accredited by ASIC
- Working closely with stakeholders to develop agreed passcode security and complaints handling standards, which is expected to legitimise existing industry safeguards and inform the ASIC accreditation approach
- Launching a communications campaign telling customers the code has changed and you are free to give your passcode to organisations that are accredited by ASIC.

Scope of data included in regime

The Productivity Commission has stated that there should be industry agreement on what data should be released, recommending that if agreement is not reached, the Australian Competition and Consumer Commission can step in and mandate data-sets, and in doing this should take the broadest definition possible[13]. The House of Representatives' Standing Committee on Economics inquiry into the four major banks (the Coleman Review) stated that banks customer's transaction history, account balances, credit card usage, and mortgage repayments should be among the data to be released. [14]

FinTech innovation comes in many forms, and requires many different data points that will differ in importance from one use case to another. Given the fact that the nature of different parties will require varying access to data, which is ultimately used to service the customer, any reduction to the variety of data provided by data aggregators currently will be to the detriment of millions of customers who are already customers of products and services delivered by fintechs and/or data aggregators.

The previous section outlined a number of phases constructed around a series of use cases that will ultimately determine the scope of data required to fulfill each use case. Data scope for phase 1 and 2 should include all data that can be currently accessed by a customer either

[13] See page 191 of Productivity Commission report at
[14] See page 59 of the Coleman Review at

through internet banking, statements, or call centres. This includes customer name, date of birth and address, particularly as relates to phase 0 regarding KYC. This should be achievable within a fairly short timeframe for 2 reasons: first, the data currently exists in electronic form, and second because customers can access this data already, and the regime simply makes it easier.

Through phase 2 and 3 in particular, all FSIs included in the regime will need to expand the scope of data relative to what data aggregators currently make available. For example, data should include customer product type, interest rate, product maturity date, whether it is fixed or variable, whether it is interest only or principal and interest, any offset details.

Ultimately, data to be released should cover the following types of accounts:

- Deposit
- Superannuation
- Credit cards
- Loans
- Investments, including ASX listed securities and retail managed funds
- Rewards/Miles
- Billing
- Insurance (Life, General, Health)
- Mortgages
- Lines of credit

Superannuation in particular represents a significant opportunity for Australia, given that Australia in 2016 recorded the world's fourth largest superannuation market valued at US$1.6 trillion and experienced one of the highest growth rates of pension fund assets in the world.

Customer data in public and semi-public control should also be able to be fetched by the customer, including share registry and Australian Tax Office information. Tax information in particular should help business lenders to more accurately price, and give access to, loan opportunities.

Standards, Accreditation and Governance

Process to determine standards

The establishment of agreed minimum privacy and security standards is a necessary first step for the successful implementation of Australia's Open Financial Data regime. This submission does propose some privacy measures and security standards that may serve as a starting point, but we recognise that some use cases will require different types of data with varying levels of sensitivity, and subsequent risk mitigation steps will need to be commensurate with security required, and other aspects of accreditation.

Much progress has already been made on the development of standards for both privacy and security in other jurisdictions - and even in the local market by players such as Yodlee, Macquarie Bank and Citi. For example, the use of OAuth 2.0 has evolved as a common security standard for the use of APIs. As such, FinTech Australia believes the standards development process could be undertaken within the timeframes as prescribed in the previous table.

FinTech Australia has long argued that a working group consisting of industry (large and small), government and consumer stakeholders would be best placed to determine these standards, chaired by a representative from both Treasury and a financial regulator (such as ASIC) to ensure that the consumer-directed policy outcomes are met in the timeline mandated. It is important that industry, particularly FSIs, should not chair this process, as there may be conflicts of duty and interest, and a disincentive for them to meet the policy outcomes in a timely manner.

Consumers' interests will be promoted most effectively if standards for permissioned access to financial account data are developed by industry specialists, based on requirements set by industry, government and consumer groups. These standards should also be regularly reviewed and updated by industry, and should not mandate a specific type of technology. Standards development is also best done by a set of stakeholders specifically selected for each phase, given the use cases are different and may require specialised industry knowledge and separate consumer stakeholder groups. Appendix 1 outlines FinTech Australia's recommendations for potential relevant stakeholders for each of the different use case phases.

Accreditation and ongoing governance

Not only must consumer financial data delivery be timely, consistent, accurate and complete, verification is also needed to ensure that the security systems and processes of all parties handling the data meet the minimum standards required. This is critical to ensure that risk and liability is manageable for FSIs, for 3rd parties receiving the information, and for the consumer.

As such, FinTech Australia's members believe that entities such as fintech companies seeking to receive and use financial data on behalf of a consumer - either directly from another FSI, or via a data aggregator - should be required to undergo an initial, one-off registration or accreditation process prior to being able to receive consumer data. The accreditation process should not be onerous; it should simply require companies to register certain information, such as their company details and relevant contact person information. In doing so, the company effectively declares that it meets the minimum required security and privacy standards for participation in the regime, as determined by the working group. Similar to the privacy act, no external or 3rd party certification should be required; compliance should be assumed, with heavy penalties imposed by the regulator on those found to be in breach of these standards.

However, a more stringent level of accreditation, or certification (as required by the Document Verification Service, for example) should be applied for large Data holders, such as Data

Aggregators, Credit Bureaus, Data Exchanges and potentially also FSIs and fintechs who hold significant amounts of data for a large number of individuals. This could potentially be applied on the basis of a materiality threshold; for example a more rigorous level of penetration testing and certification by independent testers, and/or a cyber security insurance policy requirement could be imposed for organisations that hold over 1 million unique consumer records.

It is FinTech Australia's view that any accreditation process required for entities wishing to receive, hold, or exchange financial data under Australia's Open Financial Data regime should be managed by a regulator such as ASIC. As an entity already established for the monitoring and enforcement of financial services providers, there is efficiency in this given ASIC already administers the financial licensing process that most fintech companies and other FSIs must undertake. This is preferable to having any new group administer the process, which would require additional funding and may not necessarily have consumers' best interests in mind.

As technologies evolve over time, so too do standards. In line with the recommendation prior, ASIC should also be responsible for periodically convening a security and privacy standards working group as an Advisory Group, similar to the current ASIC Digital Finance Advisory Committee and composed of similar stakeholders as proposed for the initial working group, to review and update standards and ensure they are always kept in line with best practice. Updates and changes to standards, including compliance timelines, would be treated in much the same way as updates to regulatory regimes and guides.

Registration and accreditation to minimum required standards will form a critical part of Australia's Open Financial Data regime. It will ensure that those participating in the regime are taking necessary steps and precautions to protect consumers' precious data; by ensuring compliance, fintech companies, data exchanges, data aggregators and FSIs will ensure that they maintain valuable consumer trust.

The formation of agreed minimum required standards is also important to ensure that an even playing field is created for the sharing and use of consumer data to consumers' benefit above all. The current approach of having varying, competing security standards for basic information transfer creates substantial inefficiency, and leaves the door open for institutions to continue to use their own interpretation of baseline security standards as a means to pick and choose whom consumers are able to share their data with.

Technology (the API question)

As referenced earlier, FinTech Australia's members firmly believe that any legislation for Australia's Open Financial Data regime should be technology agnostic; that is, the regime should dictate the desired policy outcome and expected consumer service experience without directly specifying the type of technology required, so it can stay relevant and continue to harness any future technological developments and advancements.

For example, legislation might focus on a set of principles:

1. Subject/customer that has the right to direct (identification and consent)
2. Accreditation/permission (who is the data going to/via, do they meet required security standards, and what level of accreditation they hold)
3. Level of access (depending on data scope required by use case, and also on 1 and 2 - data could be provided ranging from detailed raw data, through to aggregate data or answers/insights only)
4. Consumer experience (latency, accuracy, and continuity of data flow - an API-like experience or better)

For permissioned parties, including data aggregators and fintechs, some of the most significant obstacles to effectively utilising consumer data are disruptions to the flow of data, data that are unreliable, and high latency in the receipt of data from the account provider.

For consumers, these same obstacles – disrupted connections, unreliable data and outdated information – can cause more financial harm than simply confusion and inconvenience. For example, a financial decision to purchase a product based on out-of-date information about their current product holding may result in them becoming over-exposed to a particular asset class, or over-indebted beyond their capacity to repay, without their knowing.

Application Programming Interfaces (APIs) and Screen Scraping

In creating a technology-agnostic regime, considerable thought must also be given to ensuring that consumers have convenient, cost effective access to their information and tools to help them make better decisions. The Productivity Commission's report into Data Availability and Use outlined that the new comprehensive right could be achieved by enabling the sharing of machine-readable data. Machine-readable data however can be static, such as CSVs or PDFs, which can impact data usability and long-term value to the consumer.

An excellent case in point is the changes that were supposed to transform the retail energy sector over the past decade. In particular, the concept of requiring energy retailers to make standardised pricing information available to consumers, but allowing this to be done in unwieldy PDF files resident on dozens of different web sites belonging to energy retailers has made actually accessing this information and use of it by consumers completely impractical. Gaps in data, including which customers are actually entitled to access which offers, also make it difficult for consumers and other market participants to use this data.

Without significant care and consideration, it is easy to imagine the Open Banking initiative resulting in a tsunami of data being made available, but in ways that can't easily be used and that ultimately provides little or no benefit to consumers.

APIs allow for a seamless customer experience, and can provide either "one-off" or continuous, real-time information for a specified duration to consumers or their designated data receivers at the their discretion. They are a current international best practice framework for data sharing in the technology industry. They can also speed up the rate of innovation and delivery of efficiency for consumers due to their reliability and ease of use.

The UK Open Banking Implementation Entity (OBIE) tasked with developing standards and implementing the UK's Open Banking regime) posited that "open APIs be built as open, federated and networked solutions, rather than as a centralised system. This echoes the design of the Web and will allow wide scope for innovation".[15]

In addition, below are some of the broad design principles for Open Banking set by the OBIE:

- Leverage open international standards
- Apply appropriate separation of concerns
- Support evolution
- Support interoperability
- Third-party-providers (TPPs) should not be forced to support 9 different security protocols to interact with the CMA9 (major banks).

Whilst APIs are held as a best practice technology, and are already common in the industry particularly in the provision of aggregated data to permissioned parties, we re-emphasise the importance of customer-permissioned screen scraping techniques to Australia's fintech industry. Consumers currently receive benefit from the provision of real-time and near real-time information, and a high standard of user experience that comes from products powered via companies leveraging screen scraping technologies. As such, any questions of technology should consider two key factors which may impact the uptake of solutions under a new regime: Data Set Availability and Customer Experience. It also highlights the importance of formally legitimising current screen scraping aggregation whilst new technologies and frameworks emerge.

Data Set Availability

Bank data aggregators using screen scraping technology have been operating in the Australian market for many years. Such aggregators retrieve a range of data from online banking with the permission of the customer. Additional data points that can be sourced are continually being added to the data set provided by aggregators - this data provides a much deeper and more valuable view than just transaction data and high level account holder information.

For example, consider when a lender requests information concerning a consumer's financial position when applying for a credit product. If such a data set is provided by an aggregator it may include information such as existing loans, loan amounts, interest rates on loan, average

[15] Open Banking Implementation Entity Update, May 2017

repayment amounts, frequency of repayments and time remaining on the loans. With this data, a lender can make better, or more proactive decisions in regards to a consumer's financial position or financial health in line with Responsible Lending legislation.

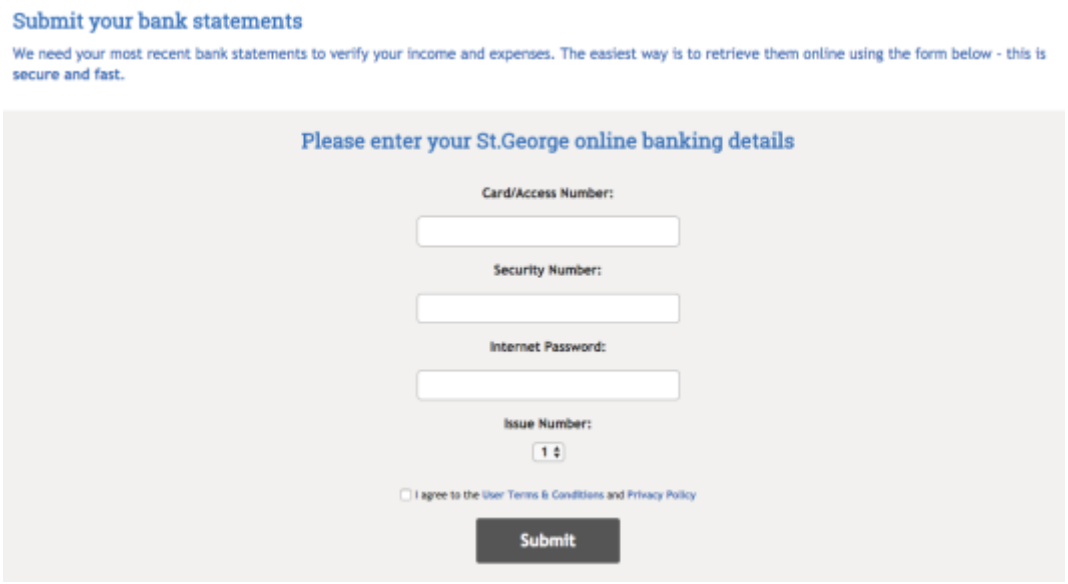
Data sets provided by banks under an Open Banking regime may not be as complete as what is currently available through data aggregators. For some participants in the fintech ecosystem, this may not matter and a feed of transaction data from the bank may be sufficient. However there will be many other participants - and their customers - who would be severely negatively impacted if the available data set was reduced in scope.

By legislating frameworks and principles for an Open Financial Data regime rather than specific technology directives, competitive market forces can continue to operate, and data sets will be increased rather than diminished which will lead to better consumer outcomes. For example, hybrid solutions between bank APIs and screen scraping data aggregators could also flourish under these frameworks.

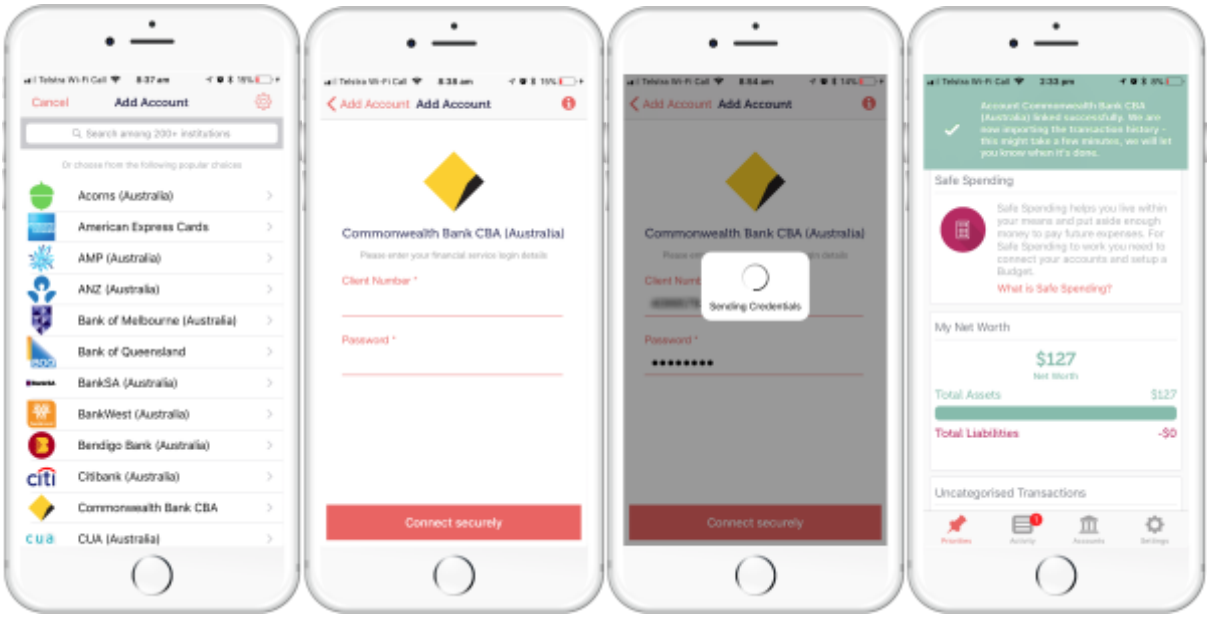
Customer Experience

Thanks to Facebook and other digital platforms, consumers are now accustomed to seamless digital experiences and are entitled to expect such from new Open Financial Data frameworks. Any increase in the friction of interaction between a consumer and a bank or fintech player to retrieve or control their data will disempower consumers from seeking product alternatives that may better meet their needs, and would limit opportunities for innovative business models in banking that could enhance competition. It can also lead to unfavourable commercial outcomes for all involved in the value chain, which will in turn lead to less investment in data sets and less data being made available. All up, the regime would fail to meet its stated policy objectives.

Excellent consumer experience is essential to ensure the success and growth of the Open Banking regime beyond launch. Most aggregators using screen scraping provide a very simple and easy to engage with customer experience. The process is typically web based and can be performed on any internet enabled device. It involves the consumer selecting their bank and then entering their online banking credentials:



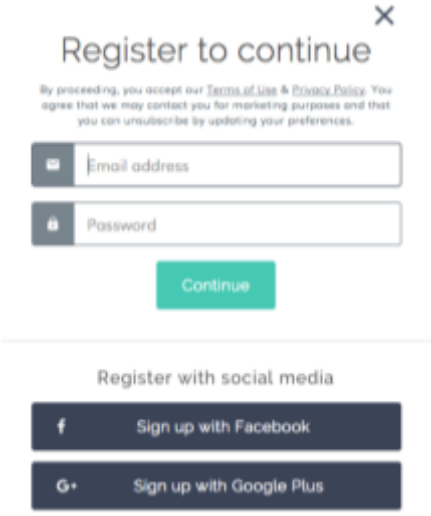
Another example:



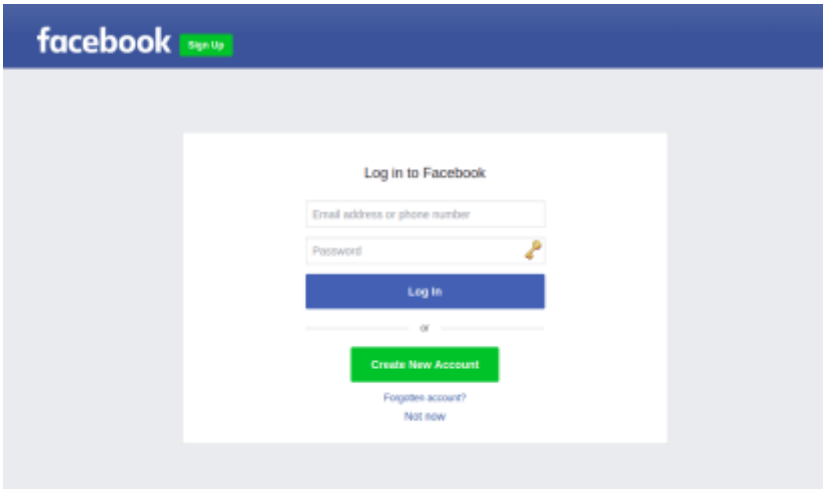
When data is captured extreme care is taken to ensure that the data remains protected in both transfer and rest. All communication is handled over an SSL (encrypted) channel and the data at rest is encrypted using encryption standards such as AES-256. The negotiation and exchange of the tokens handled during the authentication and authorisation process is done so in accordance with the OAuth 2.0 specification.

OAuth 2.0 is an industry accepted standard for authorising access to data and authenticating a consumer is who they say they are. It is also a simple, secure and straightforward experience for consumers if implemented well. Below is an example of a Facebook OAuth integration with a Fintech application:

Step 1: Consumer clicks "Sign up with Facebook"



Step 2: Consumer is directed to a Facebook-hosted authentication screen where they are prompted to log in with their credentials.



Step 3: Once authenticated by Facebook, the consumer is also prompted to confirm which data is being shared with the third party. This data is securely passed to said party by Facebook.

If consumers are required to go through more complex steps than the above, the increased friction will reduce uptake.

Consumers are clearly benefiting from a broader range of choices about the financial products and services they can use to manage their financial lives. Because many of the most effective tools in the market today rely on permissioned access to consumers' financial information, ensuring secure and reliable ongoing access to these data throughout the implementation of the regime is critical both for consumer choice and further innovation.

Digital Identity frameworks

A key facet of financial services, particularly as relates to KYC, is Digital Identity. In Australia, KYC relating to financial services is subject to regulation by the Australian Privacy Act, AUSTRAC and ASIC. There are also multiple departments within government working on Digital Identity-related solutions for a number of use cases both directly and indirectly related to financial services.

The government is currently considering a formal response to the Productivity Commission's inquiry into Data Availability and Use, particularly as relates to the Comprehensive Right for Consumers to be able to share and exercise control over their data. In particular, this is highly relevant to the work of the Digital Transformation Agency (DTA), who are currently undertaking projects in relation to Digital Identity.

FinTech Australia is very supportive of Government's attention to both the Productivity Commission's inquiry, and also to the attention toward solving the question of how a Digital

Identity framework might work in Australia. A robust Digital Identity framework will deliver significant cost reductions and efficiencies to business, and will deliver even greater efficiencies for consumers who will save time and effort when applying for financial services, which usually require onerous in-person checks and paper-based applications.

However, FinTech Australia strongly urges the government to consider its role in, and approach to the development of a Digital Identity framework. It is clear that Australia's cultural context would not permit the development of a centralised Government-built, and Government-controlled system as has been done in India via Aadhaar. The backlash against previous attempts such as the ill-fated "Australia Card" is clear evidence in support of this.

Likewise, FinTech Australia is not supportive of the notion that the Government "pick winners" by appointing a sole provider for Digital Identity, like the UK Implementation Entity has done with PingID. This effectively creates a government-backed monopoly, which will have obvious anti-competitive outcomes that may require future regulatory intervention.

Instead, we highly recommend that Australia's Digital Identity framework be spearheaded by Government (mainly as a provider of requirements and access to Government systems that may be needed), with standards that are co-developed in collaboration with industry and consumer groups specific to each industry's use case. This is especially important in Financial services, given the additional regulatory requirements that KYC entails that are particularly unique to the sector.

It is also necessary for Digital Identity frameworks to be tackled using an approach that primarily addresses standards rather than delivery of actual technology, and is in fact technology agnostic, to again allow for the incorporation of advancements in technologies (such as biometrics and other forms of authentication). The development of standards will also allow multiple vendors to compete, resulting in a more optimal end-consumer outcome.

Privacy

Privacy is a core consideration for both the design and practical application of any proposed open data regime, and in particular one that governs the transfer of sensitive customer financial information. We believe the confidentiality and integrity of financial data transferred using consumers' personal security credentials are of utmost importance.

Fundamentally the current Privacy regime has already well catered for the ecosystem proposed in FinTech Australia's submission, albeit with a number of nuances specific to the phased rollout and use cases. As Australian Privacy Principles (APPs) already stipulate consumers should be in control of their own data, open banking takes the next step and empowers consumers to share access to their financial account data securely and effortlessly.

The starting point is that Consumers must be able to easily provide explicit consent for access to and use of their data, and after consent is granted little to no impediments to the flow of data should be present (i.e. it should flow in near-real time). Industry must work together ensure that consumers are aware of, and are actively consenting to, the opportunities and risks associated with sharing their financial data, and that they have ongoing agency to renew, revoke and change their consent.

Application of APPs to participants in Open Financial Data regime

The application of the APPs under Australian privacy law currently applies to all companies with annual turnover of over $3 million. However, given the above-average sensitivity of financial data, FinTech Australia proposes that any entity wishing to receive consumer financial data under the Open Financial Data regime should voluntarily comply with all facets of Australian privacy law, regardless of their annual turnover. This would be enforceable as part of their registration or accreditation process. Similar precedent already exists, for example smaller entities seeking to work with sensitive Government data are required to proactively comply with APPs as Data obtainers.

Consumer consent and control over data

Under the current Australian privacy law regime, an emphasis is placed on obtaining consent in order for an APP entity to collect and share financial data.

Consent means express or implied consent. The four key elements of consent are:

(i) the individual is adequately informed before giving consent;
(ii) the individual gives consent voluntarily;
(iii) the consent is current and specific;
(iv) the individual has the capacity to understand and communicate their consent.

The Australian Privacy Principles:

(i) emphasise that collection, use and disclosure of personal information should be done in an open and transparent way (APP 1); and
(ii) require that the consumer be made aware when their information is being collected (APP 5).

The current Privacy law also gives an individual some control over their data. For example:

(i) the right to ‘anonymity and pseudonymity’ (APP 2);
(ii) the right to be notified if your data has been collected (APP 5);
(iii) the assurance that information will not be collected by unsolicited methods (APP 3 and 4); and
(iv) the right to access and correct personal information (APP 12).

It is FinTech Australia's view that the rollout of an Open Financial Data regime as outlined in this submission will fit well within the gambit of the APPs, and will ensure that all participants in the regime put the customer's interests at the forefront of data sharing and use. Current laws already allow for an individual to understand and give consent to a third party to use their personal financial data for a clearly defined purpose, such as making a lending decision or offering personal finance management services.

However, whilst the APPs provide a framework for an consumer to give their consent for a third party to access their personal financial data, the current law is limited around their ability to control it, for example their ability to limit the time period (e.g. once off, one month, ongoing until told to stop), and in placing obligations on an entity currently holding the desired financial data to share this with a third party if the consumer directs them to do so. It is also not currently explicit in the APPs that this control and consent framework should extend to small businesses.

It is acknowledged that in an open API context, there are different ways of structuring the relationship between the consumer, an FSI and a third party service provider. For example, one approach is that the consumer directs the bank to share its data with a third party. A second approach is that the third party obtains the consumer's consent, and directly (or indirectly via an aggregator) approaches the bank for the consumer's financial information. Under this second model, there would need to be changes in the law to clearly spell out the legal obligations and assist in the smooth flow of data, such as those recommended previously regarding the ASIC ePayments code.

A third approach also acknowledges that some consumers may also have an agent (such as a Financial Advisor or Accountant) whom they may have granted a level of proxy to. Similar considerations and subsequent mechanisms for data sharing and use as those proposed in this submission should also apply to said agents acting on behalf of consumers, with the addition of verification frameworks for those authorised to represent consumers who require assisted consent, as these are often the first targeted by bad actors.

Consumers must have the ability to control how their data is used and made available, and have the means to easily and effectively manage this in an Open Financial Data regime. For example, they should have an ability to opt in and out of methods of using their personal data easily and intuitively, and have confidence that their personal data will not be made available to others in ways they did not agree to. Consumers must also be given the right to retract access from an organisation where reputational damage, misuse or data breach could result in harm. Transparency on the use and terms of data sharing should be in plain English with the value proposition clearly communicated.

Again, any legislation around the technologies used to enable control and consent mechanisms should be based on principles, and not prescribe specific technologies. A potential precedent that could be used to as a starting point for consumer consent and control principles in

Australia's Open Financial Data regime is a framework developed by the UK National Data Guardian, at the request of the UK Secretary of State for Health, in an effort to make it clear to patients/users of care when health and social care information about them will be used, and in what circumstances they could opt out.

Known as the Seven Caldicott Principles, they include:

1. Justify the purpose(s)
2. Don't use personal confidential data unless it is absolutely necessary
3. Use the minimum necessary personal confidential data
4. Access to personal confidential data should be on a strict need-to-know basis
5. Everyone with access to personal confidential data should be aware of their responsibilities
6. Comply with the law
7. The duty to share information can be as important as the duty to protect consumer confidentiality

Developing a similar, use-case driven level of control into Australia's Open Financial Data regime will help build broad based community support for Open Data more broadly.

Quality of data transferred

Both the quality and security of personal information are fundamental assurances provided by the privacy framework in Australia.

As it currently stands:

(i) If personal information is disclosed, the information should be accurate, up to date, complete and relevant for the purpose of the disclosure (APP 10).
(ii) an organisation must take reasonable steps, having regard to the purpose for which it is to be held, to correct personal information and also ensure it is accurate, up to date, complete, relevant and not misleading (APP 13).
(iii) The organisation must also notify any third party of such amendments or corrections to personal data (APP 13).
(iv) Personal information must also be secured and protected from misuse, interference, loss and unauthorised access, modification and disclosure; or otherwise it should be destroyed or de-identified. (APP 11).

The current privacy framework requires FSIs to take reasonable steps to ensure that a customer's data is accurate, up to date, complete and relevant (bearing in mind the purpose of the disclosure to the third party), before providing the information to a third party. With data becoming more freely available for consumers to access and control under an Open Financial Data regime, it is likely that consumers will therefore take a more proactive approach to updating their information in order to make better use of it.

However, to reinforce the point discussed previously, it is very important that data be timely, accurate and provided in a continuous (real-time) manner if the consumer directs it to be so. Disrupted connections, unreliable data and outdated information provided by an institution can cause more financial harm to a consumer than simply confusion and inconvenience.

Use of consumer data

The current privacy framework deals with use solely within the context of consent. Under APP 6, organisations can only use or disclose personal information for a purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies.

The exceptions that apply most commonly are where:

(i) the individual has consented to a secondary use or disclosure; or
(ii) the individual would reasonably expect the organisation to use or disclose their personal information for the secondary purpose, and that purpose is related to the primary purpose of collection, or, in the case of sensitive information, directly related to the primary purpose.

In practice, any use or disclosure for which appropriate consent has been obtained, is generally acceptable. As outlined in the consent and control section above, we believe the Open Financial Data regime would in fact go beyond the current privacy regime, and enhance the transparency of use and disclosure to consumers.

In applying the Productivity Commission's proposed Comprehensive Right for Consumers to financial data, the new regime should allow for even greater empowerment of the consumer to direct how their data can be used to their benefit.

Breach notification

The Privacy Amendment (Notifiable Data Breaches) Bill 2016 establishes a mandatory data breach notification scheme in Australia. This amendment requires government agencies and businesses covered by the Privacy Act to notify any individuals affected by a data breach that is likely to result in serious harm.

FinTech Australia welcomes these changes, as the safety provided by breach notification amendment supports the ability to institute an Open Financial Data regime with greater consumer confidence. Our proposal to also ensure that any participants in the new regime are accredited and must also comply with the APPs no matter what size, will also ensure that breach notification practices are also applied as part of the regime.

Data Security

FinTech Australia recognises that data security is one of the keystones for the continuation of fintech innovation and further implementation of Australia's Open Financial Data regime. Security is a shared goal, and a shared responsibility. It is also key to maintaining consumer trust; consumers expect that their data is securely transferred and held when it moves from one financial institution to another financial institution, so that it cannot be accessed by hackers. They also expect secure storage of this data.

As previously outlined, FinTech Australia recommends that a temporary working group be established, comprised of government (particularly ASIC), industry and consumer groups, aligned around specific use cases. This group is best placed to determine requirements, against which industry technology specialists should establish minimum security standards that institutions wishing to participate in the regime must meet as part of their registration or accreditation process.

It is important that these minimum security standards be established, as they ensure that an even playing field is created for the sharing and use of consumer data to consumers' benefit above all. If institutions are allowed to use varied, competing security standards for basic information transfer, it creates inefficiency and leaves the door open for them to use their own interpretation of baseline security standards as a means to pick and choose whom consumers are able to share their data with.

Large FSIs should not be allowed to control the process to determine minimum security standards; there may be conflicts of duty and interest, and a disincentive for them to meet the policy outcomes as intended. Nor is the Government best placed to determine minimum security standards alone, as resource and geographical constraints make it difficult for them to continuously maintain a view of international best practice. Government is also not necessarily incentivised to create a solution that would balance practical commercial outcomes. However, government participation in the standards-setting process, particularly the Office of Cyber Security and/or the Office of Information Commission would be beneficial to the process, as standards set by the financial services sector could be used as a starting point for other industries moving toward Open Data, leading to greater interoperability and eventually greater efficiency through the economy.

Security standards should be risk based, so that security requirements match the risk posed, but do not constrain innovation. Any legislation on minimum security standards should also remain technology agnostic in order to allow for technology to be updated on an ongoing basis as needed to ensure alignment with international best practice.

As described previously, a security standard used internationally (and domestically by many in the fintech and banking community) at present is OAuth 2.0, which would be adequate for many of the use cases proposed in the early stages of the regime's implementation, and for de-identified data. As data becomes more sensitive, and as the regime moves toward phase 4 which would enable execution or initiation, other standards may be more appropriate for certain types of sensitive data or important transactions, such as NIST and/or ISO20022.

Liability

Risks and the liability for data breaches, privacy breaches and inappropriate use of customer data are often cited as barriers for implementation of an Open Banking regime. However, we see an enormous opportunity for the implementation of an Open Banking regime to clarify liability for these matters and provide certainty to all market participants.

Our view is that the Australian Privacy Principles already provide a robust framework for establishing liability in the new regime.

Further, the Open Banking regime can help to eliminate the current uncertainty and fear caused by the ASIC ePayments Code.

Key concerns with the code are:

- compliance with the code is only voluntary and not all financial institutions comply with it
- some financial institutions use it to create fear in the minds of consumers about whether their financial institution would accept liability for fraudulent activity on their accounts if the consumer has disclosed their internet banking account credentials with a third party such as a fintech business

The Open banking regime should build on these existing requirements and obligations, make compliance with them mandatory for all participants in the Open Banking regime and ensure a "common sense" approach to liability where liability rests with the organisation that has breached their obligations - particularly in the context of both the APPs, a company's registration (requiring them to comply with APPs, and the minimum required security, privacy and customer experience standards) and/or accreditation requirements.

Cost and pricing for data

FinTech Australia strongly advocates that any basic, non-proprietary (i.e. non value-added) data in scope for the regime as proposed in this submission should not cost anything to the consumer, nor the 3rd party whom the consumer has directed to obtain/receive data.

Any financial data - particularly that which is generated by customer activity, and is currently available for them to access for free (either online or via call centre), should remain free. This is

particularly true of bank transaction data, product information data, superannuation fund member statement data, etc. The expected baseline for the format (but obviosuly not the delivery mechanism) of this data would be how data is provided in standardised formats used today, such as QIF, OFX or CSV exports accessible and downloadable from the majority of Australian online-banking interfaces available to Australian consumers today.

As the regime expands to encompass further data, the working group would need to determine what data is considered raw/basic and therefore free, and the data's suitable baseline delivery format or standard.

Pragmatically speaking, we also recognise that there are ongoing costs involved in obtaining, hosting, maintaining, and securing data on behalf of a consumer. This applies to all participants in the ecosystem, particularly those who are investing resources and effort into standardising, analysing, de-identifying and making data available to others in a more digestible, flexible and/or usable format. In these instances, FinTech Australia believes it should be permissible for fees to be charged for cost recovery, and potentially further for value-added services such as data cleansing, re-formatting and standardisation across multiple data providers.

To be clear - FinTech Australia draws a line between efforts that will be made by FSIs, aggregators and fintech companies alike to *create and facilitate* a means of making basic, raw data they hold about consumers available to them to edit or share, versus efforts made to clean, standardise, analyse, or value add to data. Whilst substantial investments will be made into data storage, security etc, this is not specifically a cost incurred to ensure its provision to others; much of this investment is made to harbour and utilise data for the organisation's own purposes to begin with. It is an investment made to ensure compliance with both Australian Privacy laws and the organisation's participation in the Open Financial Data regime.

However, in the case of data aggregators, exchanges and credit bureaus (and potentially eventually by FSIs and fintechs in future), who provide an additional service in the collection, cleansing, sorting, standardising, anonymising, analysing and reformatting of data, it is entirely reasonable that these organisations should be able to charge for these value-adding services. Likewise, in the case of Aggregators and other 3rd parties that may effectively provide compliance on behalf of other institutions, it should be feasible for these organisations to charge those institutions for their service in helping them to meet their compliance obligations in lieu of their inability to make the transition on their own within the time frame.

Consumer communication and education

Australia's Open Financial Data framework will only be effective if it is utilised by customers. These are the same customers who have been taught, for many years, not to share their bank data with others, and therefore may misunderstand why they are being asked to make decisions

about doing this. Consumers may also not understand the power and value of their data, along with their rights and any safeguards which are in place.

The Productivity Commission recommended the Australian Competition and Consumer Commission (ACCC) be resourced to, among other things, educate consumers (in conjunction with State And Territory fair trading offices) on their rights and responsibilities under a new open data framework. [16] This was part of a broader finding that transparency and clear communication between all participants in the data system are necessary for maintaining social licence. The Coleman review did not touch on this issue.

While ACCC's newly established Financial Sector Competition Unit has received funding of $13.2m over four years from 2017-18, and the Australian Treasury has received $1.2 million to conduct an open financial data inquiry, it is not clear whether any of this funding will go towards communication.

A robust, nationwide communication and education campaign should be regarded as a vital component of any open financial data framework in Australia. This should go further than just informing customers of their rights and responsibilities but also seek to build enthusiasm and momentum to encourage customer take-up of the data opportunity.

Any future Open Financial Data framework should be supported by a customer-focused education campaign, funded and delivered by the Australian Government with inputs and support from Industry, and also from Consumer groups, as part of efforts to encourage greater competition and transparency in our financial system. This will also ensure that any messaging carries the strong branding and reputational benefits of the badge of government.

Conclusion

FinTech Australia thanks Federal Treasury and Mr Farrell for the opportunity to provide inputs and recommendations to the Open Banking Inquiry.

However, as indicated, if the desired policy outcome is to empower consumers with the ability to take control of their financial data, make better decisions about their financial position and ultimately improve their long-term financial health (including for small businesses), then we must take even further steps to implement a broader scope, to include superannuation, insurance and other relevant financial institutions.

It is also of critical importance that our Open Financial Data regime enables the consumer to direct an institution to act and initiate a transaction or switch products on their behalf. Without providing consumers the ability to act, in a safe, privacy-compliant, seamless and easy manner,

[16] See page 37 of the Productivity Commission report in Recommendation 5.4

significant barriers will still exist that will stop consumers from truly realising the benefits as intended in this landmark policy advancement.

FinTech Australia looks forward to maintaining a productive dialogue with Federal Treasury and the secretariat, and to contributing further inputs as required, particularly as to the next steps regarding composition and scope of any coming working groups to implement this important and transformational regime.

About FinTech Australia

FinTech Australia is the peak industry body for the Australian fintech Industry, representing over 120 fintech Startups, Hubs, Accelerators and Venture Capital Funds across the nation.

Our vision is to make Australia one of the world's leading markets for fintech innovation and investment. This submission has been compiled by FinTech Australia and its members in an effort to drive cultural, policy and regulatory change toward realising this vision.

FinTech Australia would like to recognise the support of our Policy Partners, who provide guidance and advice to the association and its members in the development of our submissions:

- Allens Linklaters
- Baker & McKenzie
- Gilbert & Tobin
- Herbert Smith Freehills
- King & Wood Mallesons
- K&L Gates
- The Fold Legal

Appendix 1: Example working group structure for KYC

FinTech Australia can also provide proposed working group structures for the remaining use cases if desired.