

Demystifying Open Banking

What it means for bankers and banks

May 2018



Demystifying ‘Open Banking’

What it means for bankers and banks

Walk-Run-Fly: there is a role for you and things to start doing today

With Open Banking regulations coming into force in jurisdictions around the world, including last week in Australia¹, it's important that Australian bankers understand what it means for them. Is it really going to challenge incumbents the way some say, and make certain business models obsolete? What do people mean when they refer to the ‘API economy’, PSD2 and GDPR? Most importantly, why should such things matter for bankers who don't work in payments or technology and perhaps find the language of Open Banking inaccessible and intimidating?

In this report, we seek to demystify all this and illuminate new perspectives. Open Banking is more than just a new set of compliance requirements, and it will require much more than just new technology. It will affect almost everyone working in banking today, and every function has a role to play in its evolution in Australia. Most importantly, while we don't subscribe to the view that banking will be turned on its head overnight, we believe that it will have profound implications for every part of the industry, and that organisations have a list of things to start doing today.

Stated simply, Open Banking refers to the opening of internal bank data and processes to external parties via digital channels. These might be customers, trusted partners or authorised third parties acting on behalf of customers. This is the general case. Specifically, Open Banking in any particular jurisdiction is defined by its scope: including the data, the processes and, of course, the range of potential external parties. Accordingly, as we discuss in the following [Appendix](#), it looks different in the US, EU and Asia, and most likely will look different again in Australia.

In Australia, the government announced with last week's budget² the formal establishment of a Consumer Data Right (CDR) to underpin Open Banking in Australia. The CDR formally gives customers ownership of their data and makes switching easier between financial institutions, first in credit cards, savings and transaction accounts, and then mortgages. Treasury designated Data61³ with authority to design technical standards, the Australian Competition and Consumer Commission (ACCC) to monitor implementation and adherence to those standards and to the spirit of the regulation, and the Office of the Australian Information Commissioner (OAIC) to handle issues related to privacy.

So long as it is done securely, unbundling bank services and data in this way will provide greater competition, improve efficiency (through accelerated digitisation and, by removing friction in transactions between companies, greater specialisation and scale), and lead to enhanced or entirely new products and services. Open Banking will have profound implications for the way financial services are delivered and the long-term viability of different business models. This logic applies not just to banking, but to almost every other industry, including energy, consumer goods, telecommunications, health care and transportation. The so-called ‘API economy’ (Application Programming Interface), is the extension of Open Banking to other domains, and the underlying motivation for many of the recommendations of the Productivity Commission inquiry on [Data Availability and Use](#) published in March 2017. This was a precursor to Treasury's [Review into Open Banking](#) (the Farrell Report), submitted to Treasury in December 2017, which focused specifically on banking. The government has declared its intent to extend the open data regime and [Consumer Data Right](#) to energy and telecommunications next.

For these reasons, described in greater detail in [Section 1](#), the topic generates considerable interest among corporate directors, strategists, technologists, regulators, economists and other stakeholders in banks and the broader economy.

¹ See [Treasury's response to the Review into Open Banking](#).

² *ibid.*

³ Data61 is an arm of the CSIRO focused on applications of data science and big data

That said, we won't go from data portability to the API economy overnight. As described in [Section 2](#), the problem is that while the technical infrastructure for truly transformative changes to banking is already possible (including widely understood and well-established frameworks for creating such things as secure APIs, data representation and transcription, digital identity, authentication and, of course, analysis and insight generation), there is considerable social infrastructure still required for that to be created. This includes regulation, customer awareness and habits, norms of industry behaviour as well as an economic or other imperative for people to change current habits. Of course, this is exactly why it is important to get started, and there is much work to be done across every part of the industry, not just by the technologists and chief data officers.

This brings us back to Second Payments System Directive (PSD2), General Data Protection Regulation (GDPR) and the Australian equivalents we are likely to soon see. It also brings us to the real imperative facing bankers, regulators, directors and other stakeholders: how to comply with evolving requirements while preparing for a future (including technology, operating model and business architecture) that may look very different. That requires more than merely meeting regulatory requirements. Walk-Run-Fly is the analogy we use for how to compete in the economy that is coming, explored further in [Section 3](#).

This report is organised into the three sections mentioned above:

1. More than just a new compliance requirement: Open Banking will transform the industry
2. Not just for technologists: there's a role for everyone
3. Walk-Run-Fly: get started today

For a brief explainer on the key terms and concepts of Open Banking, see the Appendix to this document: [Open Banking 101 Tutorial](#).



1. More than just a new compliance exercise: Open Banking will transform the industry

Most dotcoms, including Facebook, YouTube, Twitter and Google, no longer deliver their services primarily through browsers. They do so through APIs. That's why, for example, when you receive a video sent to your phone you can see the thumbnail in your messaging app, click the triangle and watch it right away. You are watching that video through an API.⁴

Imagine if you couldn't do that. Imagine that YouTube decided years ago that videos were proprietary content which they chose not to share with third parties. Alternatively, imagine they were happy to share, indeed keen to do so, but found that producing, publishing and maintaining secure and robust APIs and third-party Software Development Kits (SDKs) for multiple programming languages was just too difficult and expensive to prioritise relative to their many other initiatives.

It wouldn't have been an outlandish decision. Not that long ago, YouTube had a perfectly good business delivering video content across a perfectly good channel which they dominated: your browser. To watch a video you opened one, navigated to www.youtube.com, found the handle and watched it there.

Simple, but would you do that today? What would be the impact on YouTube's advertising revenues, or on Alphabet's market capitalisation, if you didn't? The decision to not expose their content via APIs, had YouTube made it, could have been a \$100 billion mistake.

It's a decision that banks today make every day. Of course, banks aren't media companies. They don't get their revenue from advertising, and they have security obligations that are wholly unlike those of YouTube or its parent. But while a direct comparison between the strategic imperatives of banks today and those of YouTube 10 years ago might not be possible, banks are increasingly digital businesses, and the vast majority of products they 'manufacture' (credit, advice, protection, investment) are no more tangible than a video.

⁴ You are actually watching it through a series of nested APIs: one connecting your phone's operating system to the server for your messaging app, then another connecting that server to YouTube, plus a host of other APIs connected to ancillary services, from authentication to bandwidth and display management, which combine to deliver the viewing experience.

Exhibit 1: New products and services potentially enabled by Open Banking

Model	Description	Examples
1. New services	Creating new services that access customer data from other banks and financial institutions or to extend services provided	Account aggregation, personal financial advice, personal financial management advice, tax, super, budgeting, services
2. New channels	Accessing third party audiences by placing your provider or service within another's context	Incorporating into accounting packages, Alibaba for cashflow or foreign exchange, travel, messaging payments or super
3. New utilities (aas) ⁵	Providing a new utility or service to the market to enable others	eg BBVA opening platforms and APIs to enable others, payroll/expense validation, Anti Money Laundering (AML) / Know Your Customer (KYC) validation, PayPal etc
4. New platforms	Enabling third parties to connect with banks and other services and innovate	Digital factories such as Deutsche Bank's Digital Factory, AT&T IoT, Verizon, Credit Agricole's App store.

Rise of new applications and services

Just as for YouTube, APIs enable banks to provide services to their customers that wouldn't otherwise be possible, or at least not as securely or robustly as through APIs as illustrated in Exhibit 1.

The common thread across all these new applications is the *unbundling* of existing bank products, services, data or processes, and recombining them with products, data, services or processes from someone else.

Greater convenience and security

Importantly, as discussed in [Section 2](#), much of this unbundling and recombining can already be done today, at least for services available through internet banking (IB). The mechanism is 'online impersonation' (colloquially called 'screen scraping'). It involves consumers providing their IB login credentials to a third party like Yodlee whose bots then impersonate them, login to the relevant IB account, and perform the tasks relevant to the service in question.⁶


While online impersonation is a popular workaround for many (Farrell reports that over one million Australians are estimated to use it), it is inefficient (bots need to be reprogrammed whenever a bank changes its IB interface), unstable (the services are down while this reprogramming takes place), and most importantly, extremely risky. Although customers who divulge their login credentials to an online impersonator contractually void the terms, and therefore the protections of their IB account agreement, this is untested in court. Few people know about it, and the login experience for the consumer often strongly suggests that the service is being offered in cooperation with the bank (see Exhibit 2).

⁵ asS refers to Everything as a Service - an aggregation of Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).


⁶ Note that Yodlee connects securely through APIs where banks offer them, and to our knowledge would not dispute that this is a superior approach, but for Australian banks online impersonation is a common pathway.

Exhibit 2: Do customers know that online impersonation isn't endorsed by banks?


Examples of how impersonators describe their banks, and what customers see



Impersonator 1
("Available banks")



Impersonator 2
("Add accounts")



Impersonator 3
("Supported banks")

Australian Banks

- ANZ
- Bank of Melbourne
- BOQ
- BankSA
- Bankwest
- Bendigo Bank
- Citibank
- Commonwealth Bank
- IMB Building Society
- ING Direct
- ME Bank
- NAB
- Newcastle Permanent
- People's Choice Credit Union
- St. George Bank
- Suncorp
- Westpac

New Zealand Banks

- ANZ
- ASB
- BankDirect
- Bank of New Zealand
- Kiwibank
- TSB Bank
- Westpac

Add Accounts

Add your accounts by searching or choose an account below.

Search

Add a manual account
Add a real estate account

Common Accounts

- AustralianSuper (Australia) <http://www.australiansuper.com>
- Bank Australia (Australia) <https://bankaustralia.com.au>
- Wide Bay Australia (Australia) <http://www.widebayaustralia.com.au>

1 Matching Results

- ANZ e*trade (Australia) <https://www.etradeaustralia.com.au>

[Privacy Policy](#) | [How We Protect You](#)

What is the name of your bank?

- CUA (Australia)**
webbanker.cua.com.au/webbanker/CUA
- MLC (Australia)**
www.mlc.com.au/masterkeyWeb/execute/InvHome?openform
- NAB (Australia)**
nab.com.au/
- ADCU (Australia)**
ebank.adcu.com.au/mvp352/Login.asp
- EISS (Australia)**
member.aas.com.au/Login/EI?isExternalLogin=False&isRegLogin=False
- MECU (Australia)**
online.bankmecu.com.au/dalb/ogon/cu3140/ogon.asp
- Plum (Australia)**

Back
Configure New Bank
Next

Sign in to NAB (Australia)

Please enter the same credentials used to access your online accounts at <http://nab.com.au>

NAB ID

Password

Liability for security breaches resulting from online impersonation remains unclear. While well-known providers of impersonation services are proud of their 'bank-level' security, nothing is ever risk-free. As banks have no reliable way of knowing which customers use such services, if a major online impersonator were to be hacked this could require every bank in Australia, and indeed every bank in the world, to disable all online banking services until millions of customers updated their passwords and other details. The costs of such an exercise would be above-and-beyond actual losses from fraudulent transactions.

Given the greater security, reliability and utility of appropriately designed APIs, there is no reason to continue to permit online impersonation in Australia once suitable alternatives are in place.

Unbundling and recombining – and potentially changing bank business models

However it's done, unbundling and recombining bank services creates the possibility of entirely new business models. Banks that have capabilities in the manufacture of a particular product may, for example, find new customers thanks to API-enabled channels of distribution. At the same time, they may also find themselves ceding control of large parts of the customer interface to competitors or even non-banks. Just as with insurance, we may find certain technologies, scale and data-intensive products such as personal loans and auto finance centralise in the hands of local or even global specialists.

Other players may specialise in the customer interface, finding it easier to source best-of-breed products from different manufacturers, as well as platform solutions from an increasing number of industry-wide utilities who likewise will find it easier to establish in this environment. In some cases, banks lacking a clear affinity with any customer segment may find it attractive to specialise in back-end processes and infrastructure, including cloud, cybersecurity, AML/Counter Terrorism Financing (CTF), basic customer service and account administration, and protection from financial crime. Such opportunities may be especially relevant for smaller banks servicing the increasing number of start-ups emerging to tackle specific customer segments with targeted offers such as low-LVR home loans, micro loans or cashflow-based small business loans.

Such start-ups often begin with a very particular unmet need or business proposition in mind, and may have little interest in building out all the technology, operational, security and compliance processes needed to provide financial services in Australia, particularly where credit or financial advice is concerned (including the associated licensing obligations and legal liabilities which will only become more stringent in the years to come).

Broadly speaking, we see four models emerging in this landscape, as illustrated in Exhibit 3 using the five-layer functional model of banking we introduced in our report: [Escaping the Commodity Trap: the future of banking in Australia](#). These aren't entirely new models, but Open Banking provides a pathway to digital enablement that wasn't as open before.

How can a bank, FinTech or new entrant identify the model that suits them? Exhibit 4 provides a framework for thinking about these options oriented around the degree of customer verses product orientation driving competitive advantage.

Exhibit 3: Emerging business models

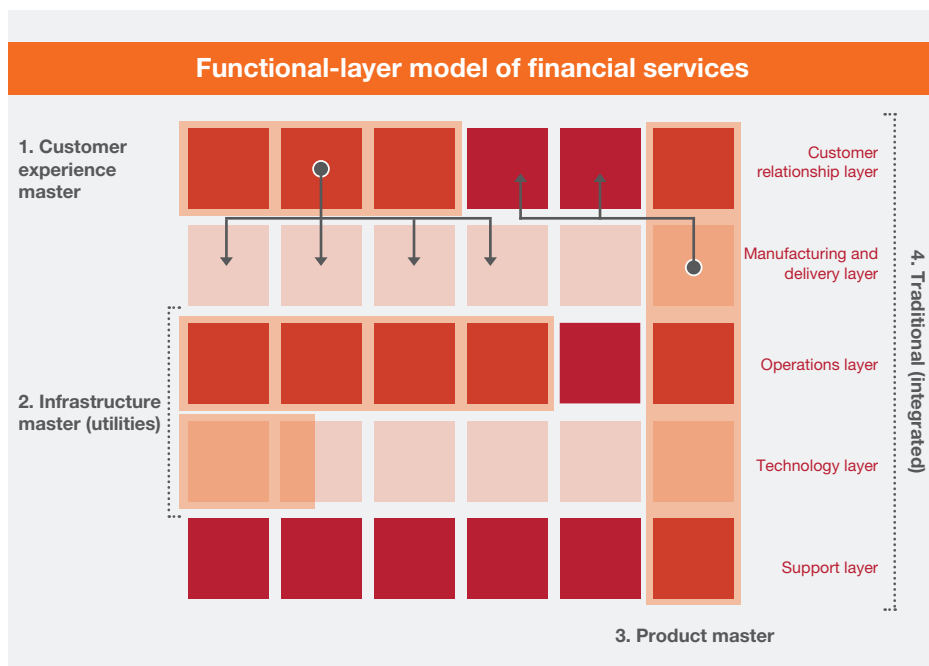


Exhibit 4: Choice of model depends on capabilities, strategy and focus

Customer relationship focus	<p>1. Customer experience master</p> <p>Players with distinct customer value proposition aligned to specific segments</p> <ul style="list-style-type: none"> • Often adjacent to banking and seeking to grow value proposition • Orchestrate 'bundle' of services to deliver digitally • E.g. Budybank, Alipay, Quicken, Treefin, online credit brokers, etc. 	<p>4. Traditional (integrated)</p> <p>Traditional banks seeking to retain control of end-to-end value chain</p> <ul style="list-style-type: none"> • Noting significant differences in breadth and depth of each specific model • E.g. Universal banks, commercial banks, credit unions, etc.
	<p>2. Infrastructure master (utilities)</p> <p>Players with distinct technology or operations capabilities that can be digitally enabled</p> <ul style="list-style-type: none"> • Often leveraging or seeking to leverage global or super-regional scale • E.g. bud, FIS, Fidor, PEXA 	<p>3. Product master</p> <p>Players with distinct capabilities that can be digitally distributed via other banks</p> <ul style="list-style-type: none"> • As with utilities, often leveraging or seeking to leverage global or super-regional scale • E.g. insurance companies, digital payment / wallet providers

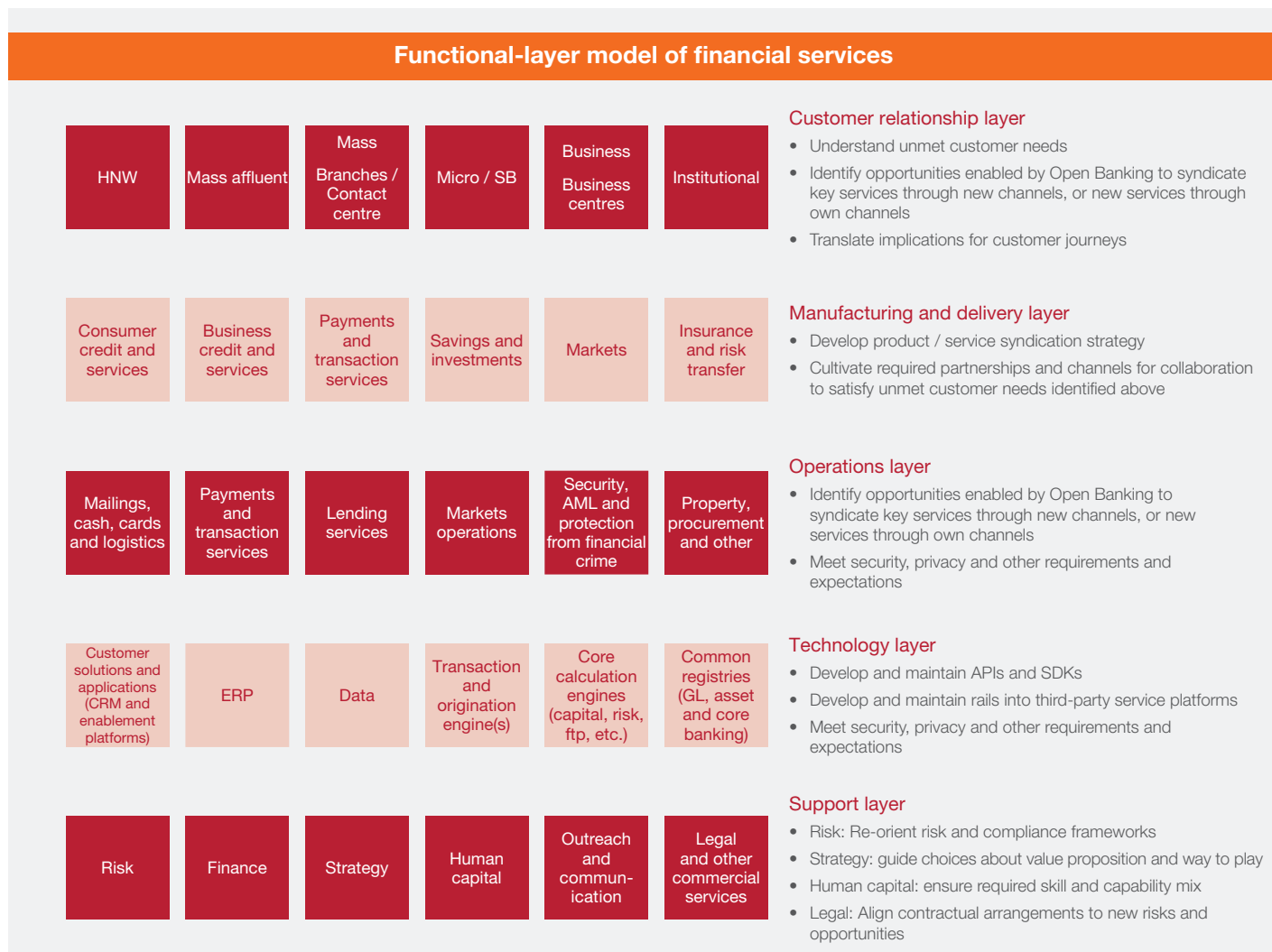
Product focus

Note that incumbent banks are currently all in the top-right quadrant – integrated providers of banking and financial services. We predict that in a world of Open Banking, many will migrate to other areas of the strategic matrix. Many executive teams and boards especially of smaller banks are already thinking about how to create a future differentiated and strategically defensible position.

However, as discussed in the [Appendix](#), we don't subscribe to the view that the future for integrated players is somehow strategically untenable or even disadvantaged. It won't be an appropriate strategy for everyone, but we expect to see large successful players surviving and thriving in the upper-right quadrant for a very long time.

In any case, regardless of the model chosen, the unbundling and recombining described here enables greater scale and specialisation. Just as in Adam Smith's pin factory, this makes everyone more successful, if they survive, but that requires deliberate choices. Banks will have to make strategic decisions about capabilities, customer needs, required investments and, always the hardest, about the opportunities they will chose to leave for someone else. This will be true for everyone in the new ecosystem, including those who chose to remain in the upper-right.

Exhibit 5: Getting ready for Open Banking: a role for every layer of the organisation



2. Not just for technologists: there's a role for everyone

Social infrastructure needed

As noted earlier, while we are confident of the changes to come, we don't subscribe to the view that these changes will happen overnight. Banking is not like riding in a taxi or using a phone. For one, much more needs to change than just the value proposition and consumer behaviour. There is still a need, especially in Australia, for what we call the 'social infrastructure' to support Open Banking.

It's not just an internal gap. Stakeholders throughout the financial services landscape will face demands for change, starting with the regulatory framework which was, quite appropriately, a major focus of the Farrell Report. Customers will also need time to understand the value proposition Open Banking enables and to change their behaviour in ways that reward investment in it.

This can be a challenge, especially in a world where there are unclear rewards for being a first mover, and where a certain 'chicken and egg' dynamic exists in which infrastructure investment requires clear use cases with compelling payback, but use cases can't emerge until the infrastructure is there.

Every part of the organisation has a role to play

Every function has a role to play in a world of Open Banking. Focusing on banks, and using the same five-layer model of Exhibit 3, we enumerate some of the things bankers will be asked to do in Exhibit 5.

3. Walk-Run-Fly: get started today?

What should the busy bank executive or director, who isn't a specialist and has hopefully found this summary informative and useful, do tomorrow?

Substantial work ahead just to comply with minimum requirements

To start, there is now a new and real short-term regulatory requirement which cannot be ignored. PSD2, GDPR and possible Australian equivalents are described in the [Appendix](#), and mean that banks still struggling with Single Customer View (SCV) even internally may find that in another 12–24 months they are expected to efficiently provide customer data to a range of third parties.

What's more, our experience in the UK suggests that technology change (i.e. the technical infrastructure) is the easiest part: agreeing standards, liability models, approaches to cooperation and other dimensions of the social infrastructure described above is far more difficult.

Fortunately, at least for the majors, readiness for PSD2, GDPR and earlier initiatives such as Comprehensive Credit Reporting (CCR) are useful precursors to the yet-to-be-defined changes following the Farrell Report. For executive teams and boards, they were also useful fitness tests of the readiness of the organisation to accommodate new data governance and access requirements. The bad news is that the timelines announced by the government are much shorter than what was available in other comparable changes to the regulatory regime.

Compliance alone is not enough

While it is not cause for alarm, we don't think a 'wait and see' approach to Open Banking anchored on merely complying with requirements is wise either. The evolution of the banking ecosystem will take time, but so will each banks' ability to respond. A 'wait and see' strategy is at risk of being hijacked by the perennial need to keep up with changing regulatory standards in jurisdictions all around the world, and another lesson from UK and European experiences in preparing for PSD2 and GDPR is that waiting until the last minute only increases the cost, risk and disruption of the change. Such a strategy is also prime for disruption by competitors who have started preparing for and understanding the new environment sooner. At the other extreme, sometimes characterisation of the scope and pace of change can border on the euphoric especially by those who have a stake in the narrative of imminent disruption – something that, in our view, is not supported by history or common sense.

Fortunately, there is a path between these two extremes. What we are calling a 'Walk-Run-Fly' approach is one where actions are more aggressive than what regulations require, but where these actions are also grounded in a sober assessment of the technical, social and commercial objective to be addressed by incumbent banks every day.

Exhibit 6: Practical compromise between denial and euphoria



Wait and see

Minimal compliance with requirements

Complying with requirements as they emerge

- PSD2, GDPR and future Australian rules
- Generally staying abreast of developments
- E.g. strategy or digital teams present regular updates to ELT

Otherwise making no unnecessary decisions or commitments

Walk, Run, Fly

Disciplined, intentional and practical steps

Ensuring compliance with all global requirements with **margin of safety**

- Staying sufficiently ahead of min requirements that no change in regulation will be a surprise
- Taking active 'no regrets' steps today even if not yet necessary

- Ready the digital and data engine
- Strengthening security and governance mechanisms
- Clarifying strategic opportunities and pathways for growth

Euphoria

Actively preparing to compete in an 'unbundled' banking

Exposing as much product and data as possible

- Customer accounts
- Transaction information
- Product

Where possible, making choices biased towards openness

- E.g. APIs with write as well as read access
- Open rather than closed APIs
- Noting that in each case significant security and privacy considerations and requirements come into play

Banks can start preparing for the commencement of Open Banking now even without knowing when compliance will be formally required. Some things banks won't regret doing include:

- Readyng the digital and data engine
 - Defining the architecture of core API libraries and data objects (which could even be industry-wide as is the case in the UK where many banks already had well-developed and widely available APIs before they were required)
 - Identifying and establishing access to critical third-party data and other capabilities
- Strengthening security and governance mechanisms
 - Defining a security, access and architecture strategy to stay comfortably ahead of all global requirements as they continue to evolve
 - Developing a strategy for dealing with the potentially commercially sensitive information that may be exposed in the new regime⁷
 - Onboarding, audit and complaints
 - Enhancing core capabilities that will be crucial in an Open Banking world, including data governance, security, identity and third-party oversight
- Clarifying strategic opportunities and pathways for growth
 - Thinking about how to compete over the long term in the new landscape, and the capabilities, assets, experiences, business models and partners needed to do so.

The good news is that many of these things are already part of existing initiatives that are spread across the banks' investment slate in digitisation, productivity, customer journeys and risk, not to mention meeting EU requirements for GDPR and PSD2. Walk-Run-Fly, in other words, does not necessarily require a wholesale change of direction. However, it may very well require a concentration of focus and acceleration of pace. The evolution of the market described above, enshrined as it is in legislation and backed by the force of regulation, is no longer optional. Customer expectations will evolve accordingly.

In summary, open banking is one more milestone in the direction of openness, digitisation and partnership with fintechs. It puts customers at the centre of the change, helping create new experiences, for them and value for the industry. Most importantly, it can be a catalyst for innovation and competition for many years to come.



⁷ For example, making transaction and other account data visible may reveal the actual interest rate charged on loans and therefore the degree of discounting being offered by each bank.

Appendix

Open Banking 101 Tutorial

Making 'internal' bank data accessible to others

Open Banking starts from the premise that customers own their data, not banks, and should be free to share it with external parties as they see fit. In its most general form, it involves opening internal bank data and processes to external parties via digital channels.

How this is done is specific to each context but, in almost all cases, participants use a core set of concepts and tools, including APIs, authentication protocols, a hierarchy of permissions and a data architecture. These are illustrated in Exhibit A1, along with a brief explanation of terms commonly used in this space.

Exhibit A1: The language of Open Banking

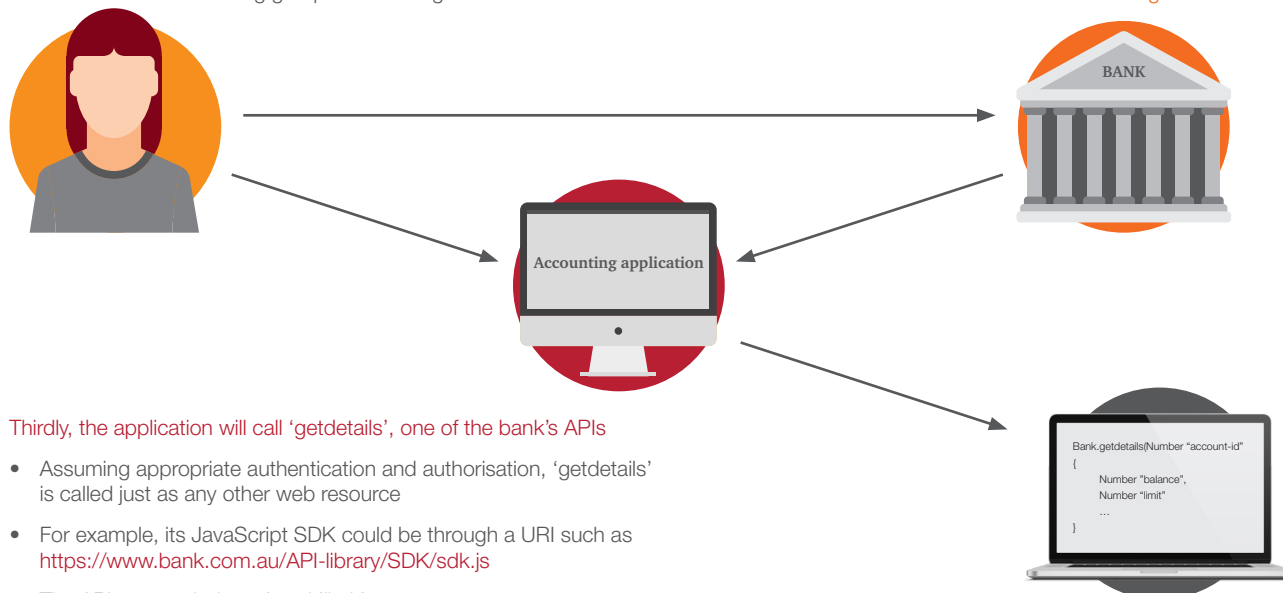
Discussions about Open Banking often include key terms which can be intimidating to non-technologists. They needn't be. For example, imagine that Jane's accounting application needs access to account information from her Bank:

First, Jane **authenticates** herself and **authorises** the app to access the needed information.

- Protocol likely a variant of **OAuth2** standard, 'state of art' for most web apps today
- Bank likely to require additional measures like **Strong Customer Authentication (SCA)** and Indirect Approval
- A group of companies - the **FAPI (Financial API)** working group - is working on this

Secondly, bank makes API code and executable available via web URI through its **SDK**.

App developer includes it in the applications code which then has access to API functions like **getdetails**



Thirdly, the application will call 'getdetails', one of the bank's APIs

- Assuming appropriate authentication and authorisation, 'getdetails' is called just as any other web resource
- For example, its JavaScript SDK could be through a URI such as <https://www.bank.com.au/API-library/SDK/sdk.js>
- The API returns 'balance' and 'limit'
- Data could be returned in a format called **JSON (Java Script Notation Language)**, which is like a .csv file for web applications
- The bank's web application (e.g. written in **JavaScript**) will know how to interpret data encoded in the JSON format

Fourthly, the bank's Digital team will boast that its APIs are 'RESTful'

That means they are written consistent with design principles proposed by Roy Fielding in his 2000 PhD dissertation

See Roy Fielding Dissertation UC Irvine, 2000

Different models all around the world

Whilst open Banking is easy to understand in principle, and the value proposition easy to imagine, it is not so easy to identify ‘killer’ use cases, especially for executives hoping to recover the cost of building an API infrastructure (including the cost of cannibalised revenue). For this reason, regulators in many markets are stepping in and forcing it to happen. In Europe, the PSD2 requires banks to expose both payments data and the ability to transact (so-called ‘read’ and ‘write’ privileges) to third parties. The national legislation came into effect in January 2018, with full operational compliance to technical standards required by August 2019. At the same time, the GDPR which takes effect on 25 May 2018 enumerates rights and obligations of banks as custodians and consumers as owners of their data. The high-level effect of these two regulations is summarised in Exhibit A2.

Though they are hardly Open Banking in the sense we described above, for the EU they are statutorily-mandated first steps. In particular, they require that banks expose the information and utility of their payments activities to third parties, potentially unbundling them from the broader banking value chain. Note that this is only one of many potential approaches to Open Banking.

In Australia, the Farrell Report proposes similar, but slightly different first steps which were embraced by the government last week. It envisages a much broader scope for the kind of customer data which should be open, but a narrower range of applications, leaving the initiation of payments (‘write’ privileges) to later stages. It also includes no explicit recommendations on privacy and security standards, preferring to defer those to a standards body which the government determined would be Data 61, an arm of the CSIRO, although it did make approving reference to certain principles such as Strong Customer Authentication (SCA). The differences between these approaches are illustrated in Exhibit A3 which schematically describes the key choices to be made when designing an Open Banking regime: what data and processes to expose, to whom, how and under what rules and governing arrangements.

Exhibit A2: The EU's first steps – GDPR and PSD2



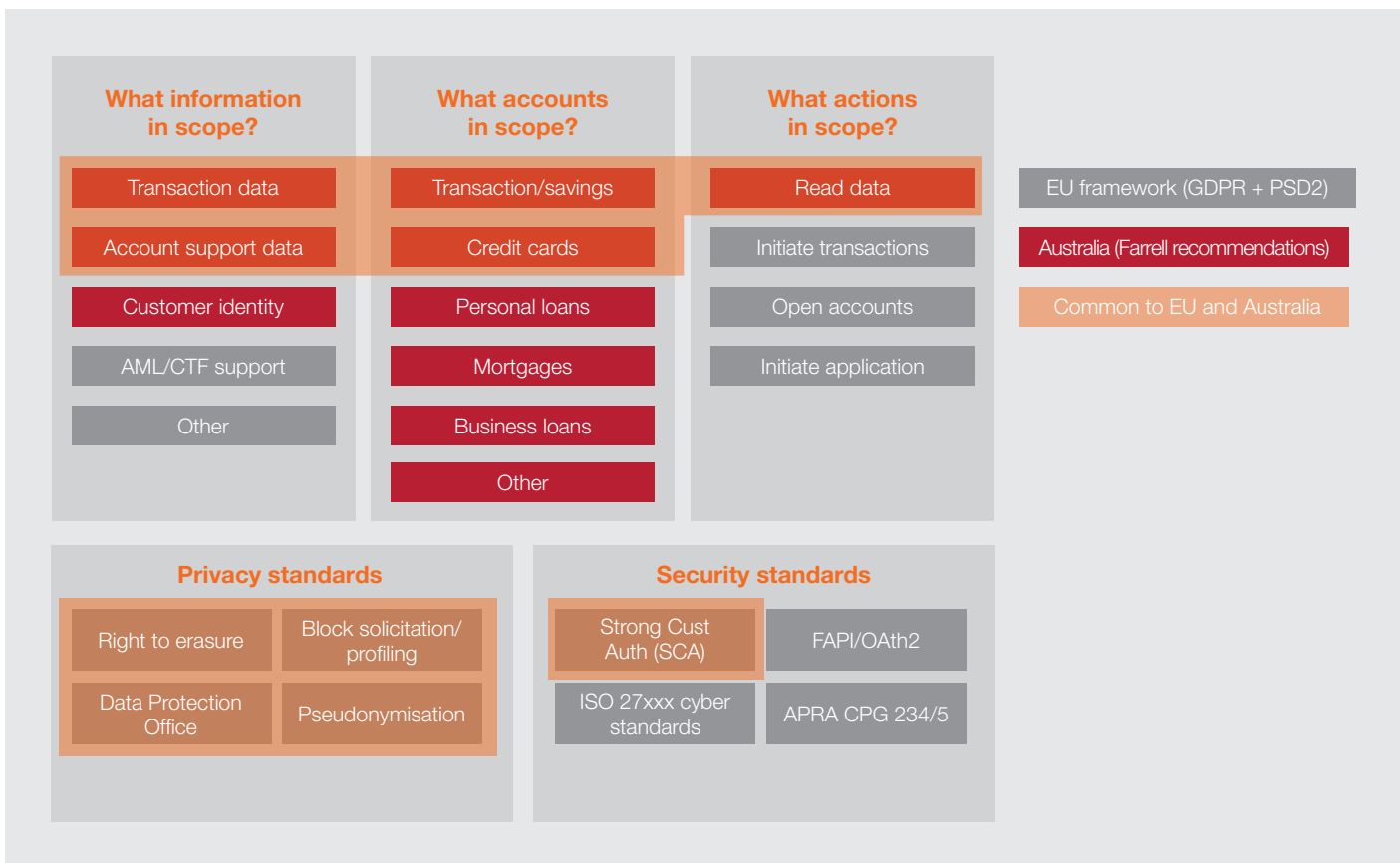
	
General Data Protection Regulation (GDPR)	Second Payments System Directive (PSD2)
<ul style="list-style-type: none"> • Takes effect 25 May, 2018 • Encapsulates three fundamental consumer rights with regard to data: <ol style="list-style-type: none"> 1. Right to be forgotten 2. Right to object to profiling 3. Right to port data to third parties • Privacy ‘by design’ <ol style="list-style-type: none"> 1. Internal data access on ‘need to know’ basis 2. Pseudonymisation by default • Sanctions for breach can be as high as 4% of global revenues 	<ul style="list-style-type: none"> • Pillar 1 (transparency of pricing and terms for payments) applies from 13 January 2018 • Pillar 2 (Strong Customer Authentication) and Pillar 3 (open access) applies from August 2019 <ul style="list-style-type: none"> – Customer authentication must comply with EU Regulatory Technical Standard (RTS) published February 2018 – Banks must provide read and write access to accounts to authorised third parties via APIs – APIs to comply with requirements published in RTS • Legislation does not prohibit online impersonation (screen scraping)

Exhibit A3: Open banking from concept to reality



Whether these differences make Australia’s implementation more or less ‘aggressive’ than the EU’s, or more conducive to innovation, remains to be seen. There are arguments on both sides. However, while GDPR and PSD2 are already coming into effect, the recommendations in the Farrell Report were only adopted by the government last week, and only for transaction accounts, savings accounts and credit cards. These must be made ‘open’ by 1 July 2019, and then mortgages by February 2020.

Of course, as international banks with EU-domiciled customers (or even payments that may originate or terminate with an EU regulated bank), Australia’s major banks must comply also with EU legislation which may influence the way Australian legislation evolves.

First era of Open Banking

Finally, no discussion of Open Banking around the world would be complete without reference to what is perhaps its first development, which occurred shortly after the invention of the World Wide Web itself. In 1997 three technology companies created an XML standard known as OFX.⁸ Through OFX and its variants, customers could aggregate and manage their financial accounts at major banks like Citibank, Bank of America and Chase, as well as other institutions such as Charles Schwab and Vanguard. They could view their accounts, initiate payments and transfers, and perform other basic account management functions. Although the specific technical architecture may have been different, it was very similar to what PSD2 promises today.

At the time, alarming claims were made that by exposing their internal data and processes to third parties, the banks had injudiciously handed control of the customer interface to the providers of Personal Financial Management (PFM) software who could then ‘orchestrate’ optimised and personalised bundles of services for clients. These new players would relegate banks to being ‘dumb’ providers of ‘utility’ balance sheet, product manufacturing and other undifferentiated services, and capture the lion’s share of value in banking - just as Microsoft had previously done in personal computing.

⁸ OFX is known as QFX by Quicken™ users, which is the proprietary OFX variant optimised for Quicken. The companies were Microsoft, Intuit and CheckFree. Microsoft and Intuit were both leading providers of Personal Financial Management (PFM) software at the time (Money™ and Quicken, respectively), and CheckFree an electronic payments services provider.

What's more, since one of those PFM providers was Microsoft (the most valuable company in the world at the time,⁹ it seemed self-evident that they had the wherewithal to develop the capabilities and assets needed to 'disrupt' the relationship between banks and their customers. How could boring banks hope to compete?¹⁰

As we know, it didn't work out that way. While the reasons for this are beyond the scope of this short survey, the lessons of the First Era of Open Banking is that while it introduced both challenges and opportunities for incumbents and new entrants alike, being an integrated provider of banking services remains a viable model even as the ecosystem has evolved. As we have argued previously, we don't expect that to change.

⁹ ...and whose CEO was famous for saying as early as 1994 that 'banking is necessary; banks are not.'

¹⁰ For its part, Intuit obtained a banking license which it has since relinquished.

Contact us



Colin Heath

Banking and Capital Markets Leader

Tel: +61 3 8603 0137
colin.heath@pwc.com



Sam Garland

Banking and Capital Markets Partner

Tel: +61 2 8266 3029
sam.garland@pwc.com



Jim Christodouleas

Banking and Capital Markets Director

Tel: +61 448 431 121
jim.christodouleas@pwc.com



Kate Eriksson

Digital and Experience Partner

Tel: +61 3 8603 0128
kate.eriksson@pwc.com



Alex Acworth

PwC Strategy & Director

Tel: +61 2 8266 4672
alex.acworth@pwc.com



Alfredo Martinez

Banking and Capital Markets Partner

Tel: +61 2 8266 5296
alfredo.martinez@pwc.com