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

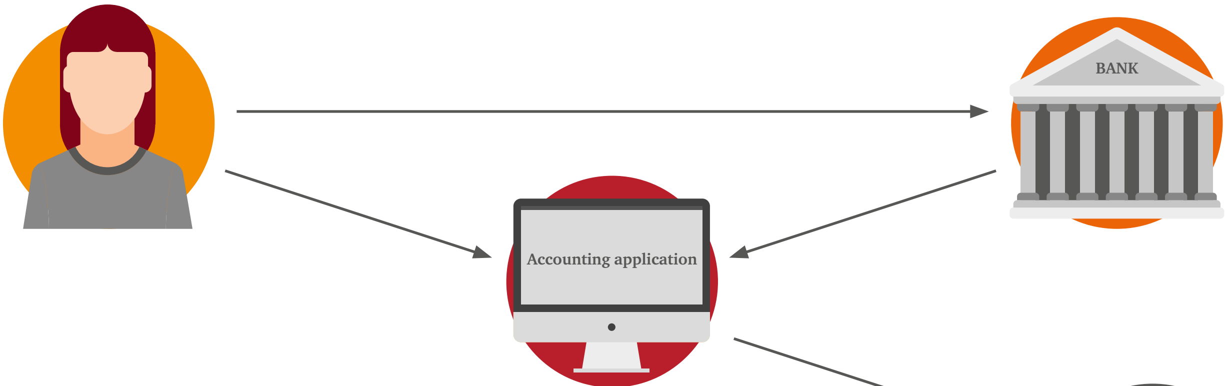
Discussions about Open Banking often include key terms which can be intimidating to non-technologists. They needn't be. For example, imagine that Jane's accounting application needs access to account information from her Bank:

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

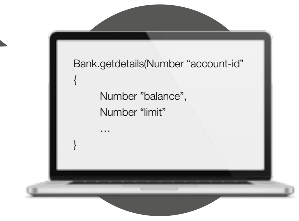
Secondly, bank makes API code and executable available via web URI through its SDK.

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 .cvs 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



```
Bank.getdetails(Number "account-id"
{
        Number "balance",
        Number "limit"
        …
}
```

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.

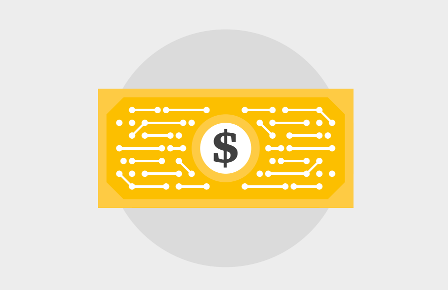
Though they are hardly Open Banking in the sense we described above, for the EU they are statutorily-mandated first steps. In particular, they require that banks expose the information and utility of their payments activities to third parties, potentially unbundling them from the broader banking value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

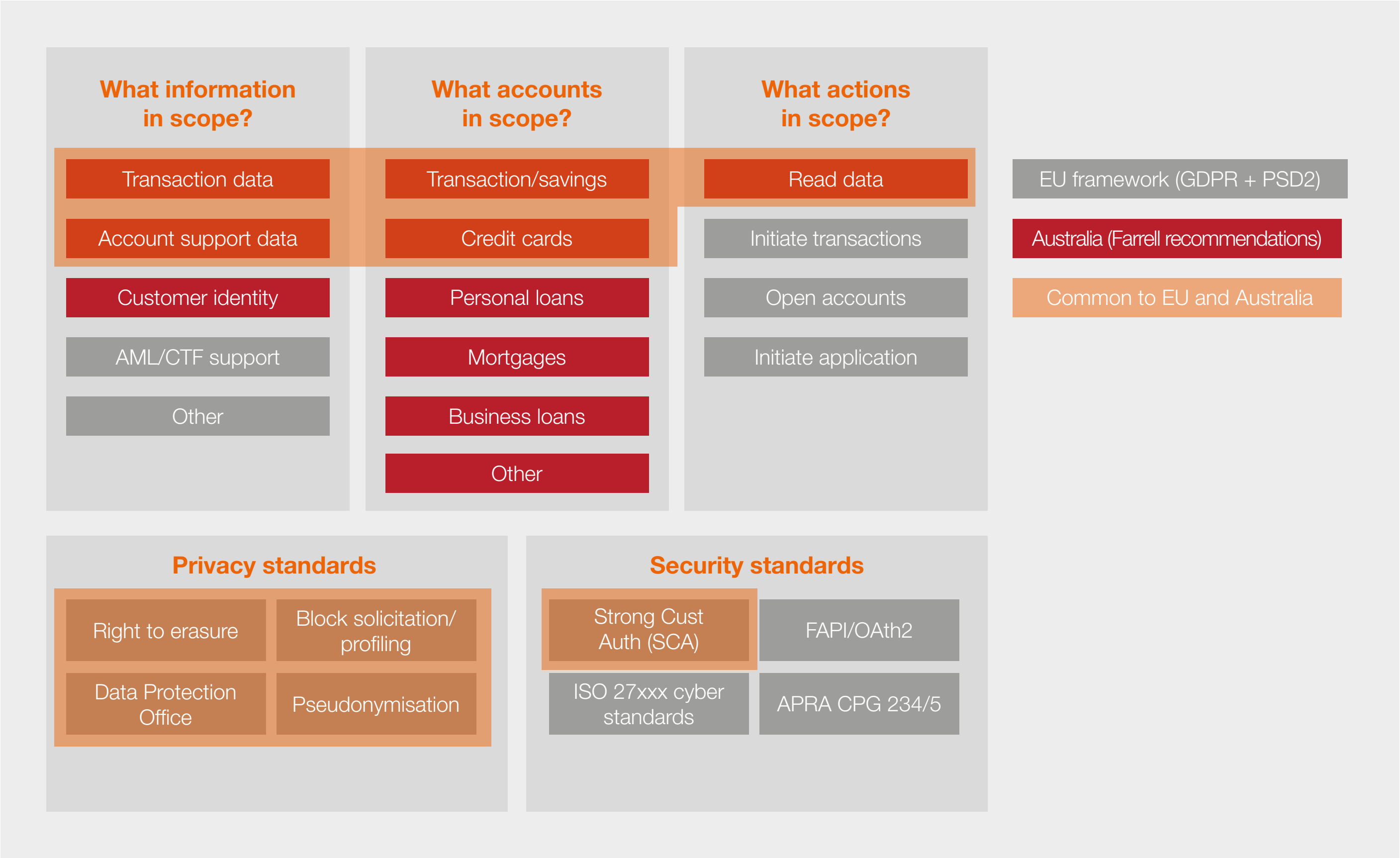
- Takes effect 25 May, 2018
- Encapsulates three fundamental consumer rights with regard to data:
    1. Right to be forgotten
    2. Right to object to profiling
    3. Right to port data to third parties
- Privacy 'by design'
    1. Internal data access on 'need to know' basis
    2. Pseudonymisation by default
- Sanctions for breach can be as high as 4% of global revenues



Second Payments System Directive (PSD2)

- 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
    – 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 conduce 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
Head of Innovation

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

Alex Acworth
PwC Strategy& Director

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

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.
Liability limited by a scheme approved under Professional Standards Legislation.
127059630