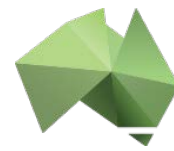




Submission by the Australian Payments Council to the Treasury Review into Open Banking in Australia Issues Paper

September 2017



The Australian Payments Council

The Australian Payments Council (**Council**) fosters the ongoing development of the Australian payments system to ensure it continues to meet the changing needs of Australian businesses and consumers with innovative, secure and competitive payment services. We are pleased to provide a submission to Treasury's *Review into Open Banking in Australia* in this capacity.

The Council was established by the Reserve Bank of Australia (**RBA**) in 2014 to guide the strategic direction of the payments industry. The Council engages directly with the RBA's Payments System Board (**PSB**) to create a shared vision and to ensure alignment between the payments industry and the PSB on significant payments initiatives. The Council's role is to:

- Drive the strategic agenda for the Australian payments system
- Engage with the Payments System Board on setting and achieving strategic objectives
- Identify strategic issues and emerging trends through constant scanning of the payments environment
- Generate common industry positions for action and adoption by the industry with the endorsement of the PSB
- Identify and remove any barriers to innovation through collaboration

The Council has an independent non-executive chairman and 13 members¹ drawn from a broad community of payments organisations. These organisations include the RBA, financial institutions, card schemes, major retailers, other payment service providers and financial technology companies.

The Council is supported by a Community of more than 30 organisations comprising technology companies, consulting firms, credit unions and mutuals, international banks, and retailers. Members of the Community are directly involved in the work of the Council, participating in project focused task forces. Over the last year these task forces have met in excess of 25 times on a range of topics, from data sharing to digital identity and cyber security. Additionally, Community members are directly represented on the Council by their elected representatives.

The Council's Innovation Agenda

With the goal of articulating a shared vision and providing strategic direction for the payments industry, the Council published the Australian Payments Plan² in December 2015. Produced in consultation with over 60 organisations and individuals, the plan anticipates a period of rapid change, driven by the demands of an increasingly digital economy. Importantly it identifies three focus areas that require collaborative action to ensure that the payments system continues to meet the desired characteristics of resilience, efficiency, accessibility and adaptability. These focus areas are:

Security and Trust to identify and promote initiatives that will ensure the continued development of a secure and trusted payments system.

¹ <http://australianpaymentscouncil.com.au/meet-the-council/>

² <http://australianpaymentscouncil.com.au/wp-content/uploads/2015/12/Australian-Payments-Plan-December-2015.pdf>

Managing the Payments Mix to ensure the evolution of a modern payments system that meets the needs of all users of the system.

Enabling the Future to support the technology innovation required to underpin the evolving needs of consumers and business. Following a scenario planning session facilitated by PwC in early 2016 to guide prioritisation, activity relating to Enabling the Future has centred squarely on giving customers greater access to and control over their payments data. In this respect, the Council's objectives are aligned with the terms of reference of the Open Banking Review.

For clarity, payments data is broadly defined as any data collected and stored electronically when a payment occurs. This data is generated when a payment is initiated via:

- Credit/debit card transactions
- Electronic funds transfers: direct debits, direct credits, internet banking Pay Anyone, mobile payments
- Mobile Wallet Transactions
- Cash withdrawals and deposits
- ATM Withdrawals
- Cheque Transactions

Over the last 18 months the Council's Data Task Force has led a series of activities designed to lay the foundation for giving customers access to and control over their payments data. These activities include:

- Development of principles for data sharing in the payments sector.
- Consultation with the Open Data Institute (the ODI was instrumental in developing the UK's Open Banking framework) including the hosting of an industry roundtable, involving Treasury, Fintech Australia, the Council and the RBA.
- Hosting a challenge design workshop as a precursor to an industry wide hackathon.
- Hosting a data sharing hackathon in Sydney and Melbourne inviting a diverse set of participants to Improve the Lives of Australians with data.

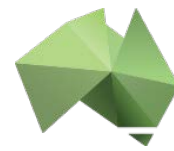
Based on work undertaken and specifically addressing questions raised in the terms of reference, the Council offers the following commentary, in the context of a whole-of-economy data sharing regime.

The mechanisms for sharing data should be principles based, rather than technologically prescriptive.

Principles help to define the parameters of action and help guide behaviour; it is for this reason that the Council's first initiative on this subject sought to develop principles for data sharing.

These principles were published in November 2016³ and are provided below.

³ <http://australianpaymentscouncil.com.au/wp-content/uploads/2016/11/Australian-Payments-Council-Annual-Review-2016.pdf>



Principles of Data Sharing

1. Consumer Privacy	Data providers and data recipients will adhere to the Australian Privacy Principles in order to protect the privacy of individuals when sharing data, notably the following principles: <ul style="list-style-type: none">• Use or disclosure of personal information• Open and transparent management of personal information• Security of personal information
2. Safe Management	Appropriate technical and organisational measures must be taken to ensure authorised and lawful processing. Data recipient must be appropriately accredited to ensure that personal information will be sufficiently secure.
3. Clear Use	Data recipients must clearly indicate their intended use of data and adhere to this.
4. Duty of Care	Data providers have a duty of care to the data owner to ensure to the best of their ability that the data recipient is acting in their best interests.
5. Lawful Use	The sharing and use of data by both the data provider and recipient must be lawful and restricted to the purpose the data was requested for.
6. Storage and Expiry	Data recipients must specify the length of time any data will be retained for. When requested data is no longer required it must be securely expunged by the data recipient.
7. Accuracy and Completeness	Data providers must take steps to ensure that information provided to a data recipient is accurate, up-to date, complete and relevant.
8. Accessibility and Usability	Information must be accessible and useable by a data recipient. Data providers must make data available in commonly used formats.

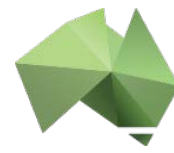
Technology mandates run the risk of creating barriers to entry and may lead to the adoption of obsolete practices. Carefully crafted principles provide sufficient detail to ensure appropriate consistency, while at the same time leaving room to encourage continuous technological advancement.

This point is reflected in the industry's identification of the need to make data available in commonly used formats; it is anticipated that these formats will change over time.

This recommendation is consistent with the recommendations of the 2014 *Financial Services Inquiry*⁴ (the Harris inquiry) and the Productivity Commission's Inquiry into *Data Availability and Use*.⁵

⁴ *Financial Services Inquiry* (2014) http://fsi.gov.au/files/2014/12/FSI_Final_Report_Consolidated20141210.pdf Recommendation 39

⁵ Productivity Commission, *Data Availability and Use* (2017) <http://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf> Recommendation 5.2



The safe provision of data to a third party requires the accreditation and ongoing management of third parties.

Accreditation plays an important role in ensuring that data providers are able to meet their duty of care to customers. It also plays an important role in engendering consumer confidence in data sharing.

An accreditation framework is agnostic as to the level of access that an accredited third party will receive. For example, a 'white list' approach could form the basis of an approved list for bilateral or multilateral agreements. Its primary purpose is to ensure that only appropriately accredited organisations are able to receive sensitive customer data.

This is consistent with the approach outlined in the EU's Payment Services Directive 2 (PSD2)⁶, which offers some useful guidance regarding accreditation, noting the requirement for third parties to provide (among other things): a business plan, evidence they hold capital, insurance (when required), governance arrangements, procedures for security incidents, processes to handle sensitive information, security policy documentation, AML controls, suitability tests.

The Council offers its assistance to Government in the development of an appropriate framework.

A co-regulatory regime supports compliance and innovation.

Frameworks to support access regimes are comprised of two distinct components:

- Establishment of rules for accreditation and governance
- Application of these rules to participants, and management of compliance issues

The payments system in Australia, which functions in a co-regulatory regime with responsibility for different areas shared between the RBA and industry, provides an interesting and relevant model. The continuous improvements of the payments system and the increased choice in terms of products and services offered to consumers illustrates how this model is able to deliver system wide improvements, while safely managing risk.

With respect to administering the provision of data, it is envisaged that the Government could play a valuable role in setting rules and threshold agreements, while the industry might reasonably be responsible for managing and reporting on operational compliance.

⁶ Payment Services Directive 2, Article 11 (Granting of Authorisation), <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366>

Focusing on Consumer Outcomes is Vital.

One of the key learnings that Council members gained from the roundtable with the ODI was that focusing on consumer outcomes and in tandem, consumer education is vitally important. This is true with respect to supporting the initial launch of services, as well as to the ongoing management of customer expectation. The Council understands from discussion with the ODI that the customer mind set and expectations were considered comparatively late in the UK proceedings.

For this reason, the focus of the recent industry hackathon was on Improving the Lives of Australians with Data. As such, the hackathon sought to generate awareness around the value of data, focusing on positive consumer outcomes. Interestingly, with respect to the Review's terms of reference, participants used payments data to develop new banking services (e.g. financial inclusion, crowd sourced savings) and new non-banking services (e.g. personal financial management tools, loyalty, and services for financial assistance in natural disasters).

Importantly, the hackathon proved to be a landmark event in industry collaboration, bringing together more than 120 developers, designers and innovative thinkers from across 4 states; NSW, VIC, SA, QLD.

A full report of the hackathon is [attached](#).

Informed Customer Consent is Crucial.

Informed customer consent is an important corner stone of providing customers with greater access to and control over their data. It is a particularly nuanced topic for payments data given the widespread practice of joint account ownership and the requirement to consider co-owner consent. Financial service providers currently manage consent mechanisms through bilateral partnerships. Careful consideration must be given to how these mechanisms might operate at scale to ensure that customers are aware of the scope of the consent they are giving. Of equal importance, customers must be able to revoke consent in a secure and convenient manner.

In many cases customers 'expect' that their data is secure, but may be unclear as to precisely what they are consenting to be disclosed to third parties. This could lead to areas of contention about who is legally responsible and accountable for the data that is shared. Similarly, customers will continue to view their bank as the repository of their personal data, and expect that financial data provided by their bank to a third party will be protected to the same standard.

The experience of the EU General Data Protection Regulation (**GDPR**) is instructive. Coming into force in May 2018, the GDPR is designed to harmonize data privacy laws across Europe, protect and empower all EU citizens data privacy and reshape the way organizations across the region approach data privacy⁷. Organisations in breach of GDPR face heavy fines – up to 4% of annual global turnover or €20 Million (whichever is greater).

⁷ <http://www.eugdpr.org/>

The GDPR strengthens conditions for consent. The request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided using clear and plain language. It must be as easy to withdraw consent as it is to give it.

The requirement for customer authentication is closely linked to the question of consent. Again, the EU's PSD2 provides some helpful guidance around the requirement for "strong customer authentication".

The Council has started to consider customer authentication in the scope of early work completed on a digital identity framework and as part of this we have mapped customer journeys for data sharing. The customer journeys are helping with the identification of elements of the framework that require collaborative action to ensure interoperability and a consistent customer experience. As the Council progresses work in this area, we will provide further information to Treasury.

Implementation.

The Council recommends a phased and iterative approach to implementing open banking, with timelines flowing from an agreed set of outcomes.

Advocating a principles-based approach, the Council offers its assistance with the development of principles as a foundational step in providing customers with access to and control over their payments data.

ENDS



Hackathon Report

Improving the lives of Australians

The Hackathon

The Australian Payments Council held a hackathon in August 2017 to examine how greater access to data could improve the lives of Australians.

A sandbox was provided that made a mixture of simulated and real data available. Participants were given from Friday evening until Sunday afternoon to address the challenge:

How can we use transactional data to improve the lives of Australians either:

- *In my daily life*
- *In unforeseen circumstances*

The Australian Payments Council's objectives were to:

- Present industry's ability to work collaboratively
- Highlight requirement for security, privacy, and consent
- Identify data sets that have inherent value
- Identify potential cross industry use cases of transactional data

When

Friday, 11 August 2017 – Sunday, 13 August 2017

Where

Stone & Chalk, Sydney

Cognizant Collaboratory, Melbourne

Who

Over 120 participants across the 2 venues formed 22 teams, some were formed prior to the event, with others formed on Friday night.

Participants came from a wide range of organisations including financial institutions, consulting firms, fintech and university students.

Objective – Collaboration

Present industry ability to work collaboratively

The following 12 members of the Australian Payments Council financially supported the event:

*ANZ, Bendigo Bank, Coles Financial Services,
Commonwealth Bank, Cuscal, NAB, eftpos, Mastercard,
Reserve Bank of Australia, Suncorp, Tyro, Westpac*

Supporters provided judges, mentors, and entered their own teams.

Event:

In attendance were over 120 individuals, from a wide range of organisations, including financial institutions, consulting firms, fintech and university students.

22 teams were formed across Sydney & Melbourne, some were formed prior to the event, with others formed on Friday night.

Multiple teams contained members from several financial institutions as well as independent participants

#datacollab

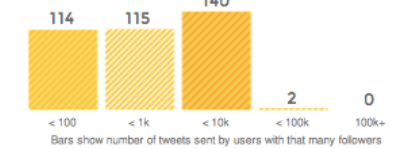
ESTIMATED REACH

80,269

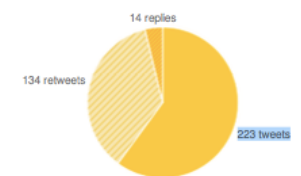
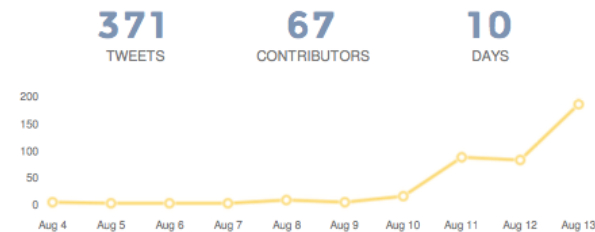
ACCOUNTS REACHED

EXPOSURE

461,183 IMPRESSIONS



ACTIVITY



Objective – Data

Identify data sets that have inherent value

Data-sets made available to all teams via sandbox included information on:

- Generic simulated product / account information
- Simulated transactional data
- Real ATM and Branch information

Event

- Wide use of transaction history in almost every application
- Personal benefit focus of challenges reduced applications looking at branch and ATM information
- No product information was used by the teams



Accounts

Access the user's list of accounts and account information such as the balance. Explore...



Transactions

Access the transaction history and metadata of accounts. Explore...



Counterparties

Access the payers & payees of an account including metadata such as their aliases, labels, logos and home pages. Explore...



Branches, ATMs

Access the list of branches and ATMs for the specified bank including geolocation and opening hours. Explore...



Metadata

Enrich transactions and counterparties with metadata including geolocations, comments, pictures and tags (e.g. category of spending). Explore...



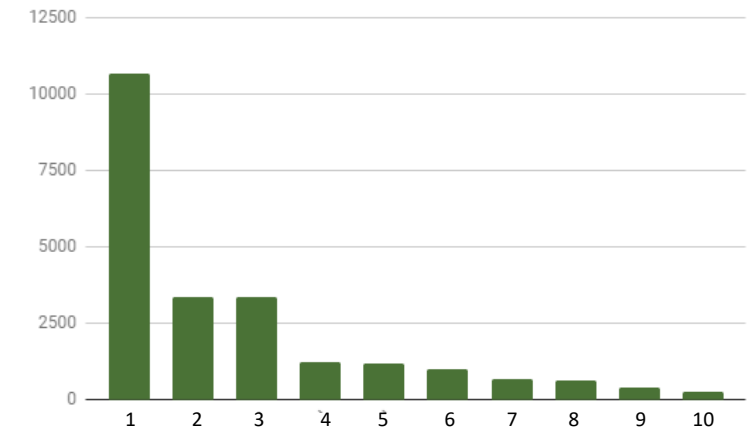
Entitlements

Enable account holders to grant fine-grained access to third-party users and applications. For instance, a business account might provide auditors with full read-only access whilst coworkers might only see the account balance. Explore...

Most used API calls:

1. List transactions for an account
2. Specific account information
3. Retrieve counterparty accounts for a specific account
4. List all available banks
5. List customers current accounts

Most Frequent API calls



Objective – Security, Privacy & Consent

Highlight requirement for security, privacy and consent

All supporting organisations recognise the need for sufficient application security, and treating customer privacy and consent with the upmost importance.

None of the data available during the event contained personally identifiable information, this allowed teams to reduce their complexity as a result teams were able to focus solely on developing and presenting a prototype. This was necessary due to the short sprint that the hackathon occurred within.

The below assumptions were required in order to make the event a success

Security & Privacy

Heavily dependent on technical implementation these were removed from the requirements to reduce specialist skills required within each team. Any real world applications should be accredited to ensure they meet a minimum level of security and privacy.

Consent

The applications assume customer consent to make their information available. In an open banking regime consent is likely to be controlled outside of the application receiving the data.



Objective – Use Cases

Discover cross industry use cases of transactional data

Over the weekend, the 22 teams started over 80 unique applications – the majority of these applications had been abandoned by Sunday night – all but 1 team was able to present a working prototype to the Judges.

The use cases observed can be broadly categorised into Banking and Non-banking products, with a number of subcategories within non-banking:

Banking

Crowdsourced savings, sustainable banking and financial inclusion

Non-banking applications

Financial coaching, loyalty, and personal financial management

Niche

Niche applications focused on what we perceive will have interest from a narrow set of consumers these applications focused on:

Dating and cryptocurrencies

Public good

Public good applications are unlikely to profit greatly, these focused on:

Natural disaster recovery, and seamless charity payments



Word cloud of submission classifications



List of Submitted Applications

A full list of all team names and submitted applications, described in the team's own words

- **Poynts** - Loyalty program on blockchain
- **SYNDICATE** – Save for your first house with family
- **Data Dating** – Dating app based on transactions
- **Odecee Hackers** – Improving bad spending habits
- **Care-net** – Power transparent donation
- **iDeal** – Discover relevant deals & benefits
- **little bit o good** – Acorns for charities
- **ONYASA** – Geo location based spend advisor
- **PurchaseBitcoins.Online** – The easiest way to buy crypto-currencies
- **Iceberg** – Monitoring customers behavior and reward with personalized discounts
- **DataCoin** – Personal bank assistant in your language
- **emFUND** – Peer-to-Peer giving for natural disasters
- **Team Opium** – Rewarding virtual wallet for sharing transactional data and personal information
- **Shooting Unicorns** – Dating app using transactions to help people find love
- **Frugl** – Gamify your spending. Optimise your savings. Compete with financial peers
- **BlazePay** – Identify and help people affected by natural disasters
- **Dot** – Mental health meets machine learning
- **SolutionZ** – Personal finance management
- **Earth** – Sustainable banking
- **Meeco** – Match available merchant loyalty programs

Winning Teams & Applications

emFund

Melbourne Winner

Origin (team size)

Syndicate Team (5)

Members from ANZ, NAB, Independent

Type

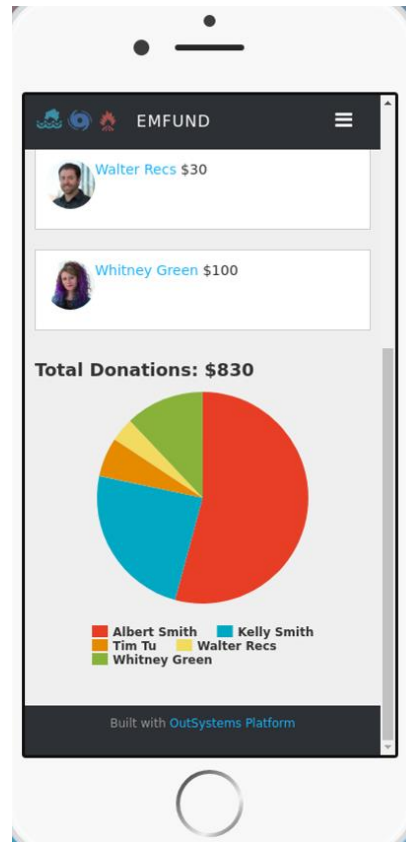
Public Good – Disaster Recovery

The App

emFund came up with a practical solution for helping people caught up in a natural disaster such as a bushfire, to access emergency funds from friends and family.

If given more time

Would tie in to distribute funds out of unaffected (cross bank) ATMs and incorporate with Facebook's Safety Check



Meeco : Loyalconception

Sydney Winner

Origin (team size)

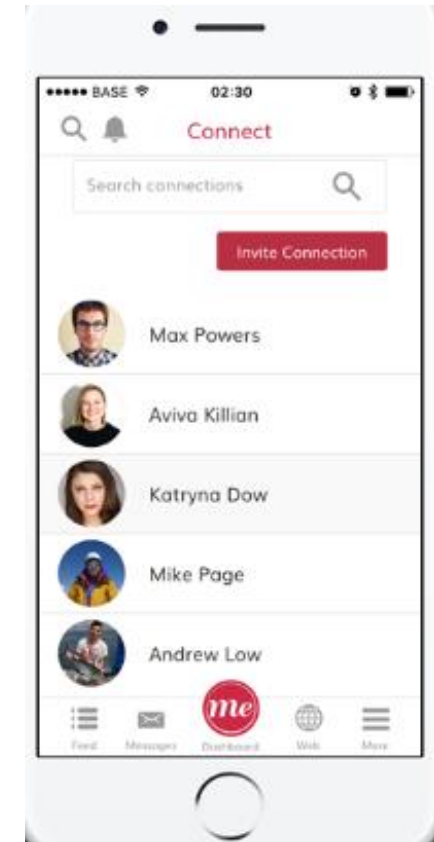
FinTech: [Meeco](#) (6)

Type

Financial Product - Loyalty

The App

Meeco used transactional data to help customers with their everyday spend. Acknowledging that there are multiple and confusing loyalty schemes on offer, the prototype analyses transactions across all the customer's accounts and identifies the genuinely rewarding offers and programmes.



Challenges & Judging Criteria

Use transactional data to improve the lives of Australians either:

In my daily life

or

In unforeseen circumstances

Teams and applications were judged on how well they met the challenges

Innovation

Is the idea innovative or we have seen it before?

- A wide variety of innovative applications were presented on Sunday, some using machine learning with others introducing voice interfaces.
- A number of applications were a fresh take on existing ideas, using round-up micro-transactions for charity or group saving.

Completion

How much progress has been made since Friday?

- The overwhelming majority of teams had working applications to present Sunday night.
- Some teams had future roadmaps for their ideas, integrating into other data sources or using more of the data provided for the event.

Viability

Is the idea viable as a long-term business?

- Ideas were broadly viable monetized through phone app stores or sold as separate products to the users.
- Some applications would struggle to post a profit but could be developed as utilities for the public good.

Use of Data

To what extent is the available data leveraged?

- The data used was mainly personal data sets (i.e. transactional data and customer information).
- No team made applications focused solely on ATM or Branch information, some felt it would be useful in later iterations as an enhancement.

Constraints & Lessons

Data

Constraint: The data sets provided to the teams was small, as a result, machine learning algorithms as well as other pattern matching applications were mocked up.

Lesson: *In future a larger production-like anonymised data-set could be used to broaden the potential uses of data.*

Available Information

Constraint: One team expressed a desire to access the component items within a purchase (shopping cart details or SKU).

Lesson: *As Financial Institutions do not have this information, it could be included by partnering with a wider range of organisations. Additional data sets could then be leveraged by participants, allowing richer applications to be developed.*

Length

Constraint: The event was a short sprint, over a weekend. As a result teams focused their efforts on presenting conceptual applications. Assumptions included: consent was provided by the customer; Privacy and security would be addressed later in development.

Lesson: *Longer future events could allow privacy, security, and consent to be evaluated in greater detail.*

Challenges

Constraint: Challenges were focused on improving an individual's experience. As a result the vast majority of applications developed used customer transaction information.

Lesson: *By broadening the challenges presented applications developed may incorporate more organisational level information (e.g. ATM, branch or product information).*

Event

- Hackathon was successful in demonstrating collaboration within the industry as a response to open data.
- Cross industry use cases shown.
- Practical observation of data sets used.
- Some desired outcomes were difficult to examine in depth due to structure of event, potential to be built on through future activities.

Recommendation

- Use current sandbox as basis for creation of a utility.
- Adjust parameters for future activities to further explore open banking:
 - Length – Extend duration of event to allows more complex topics, including consent, security and privacy, to be addressed
 - Data – Provide additional richer data sets, to allow further cross industry collaboration
 - Challenges – Present alternative challenges, focusing teams to explore use of different data sets



Australian
Payments Council