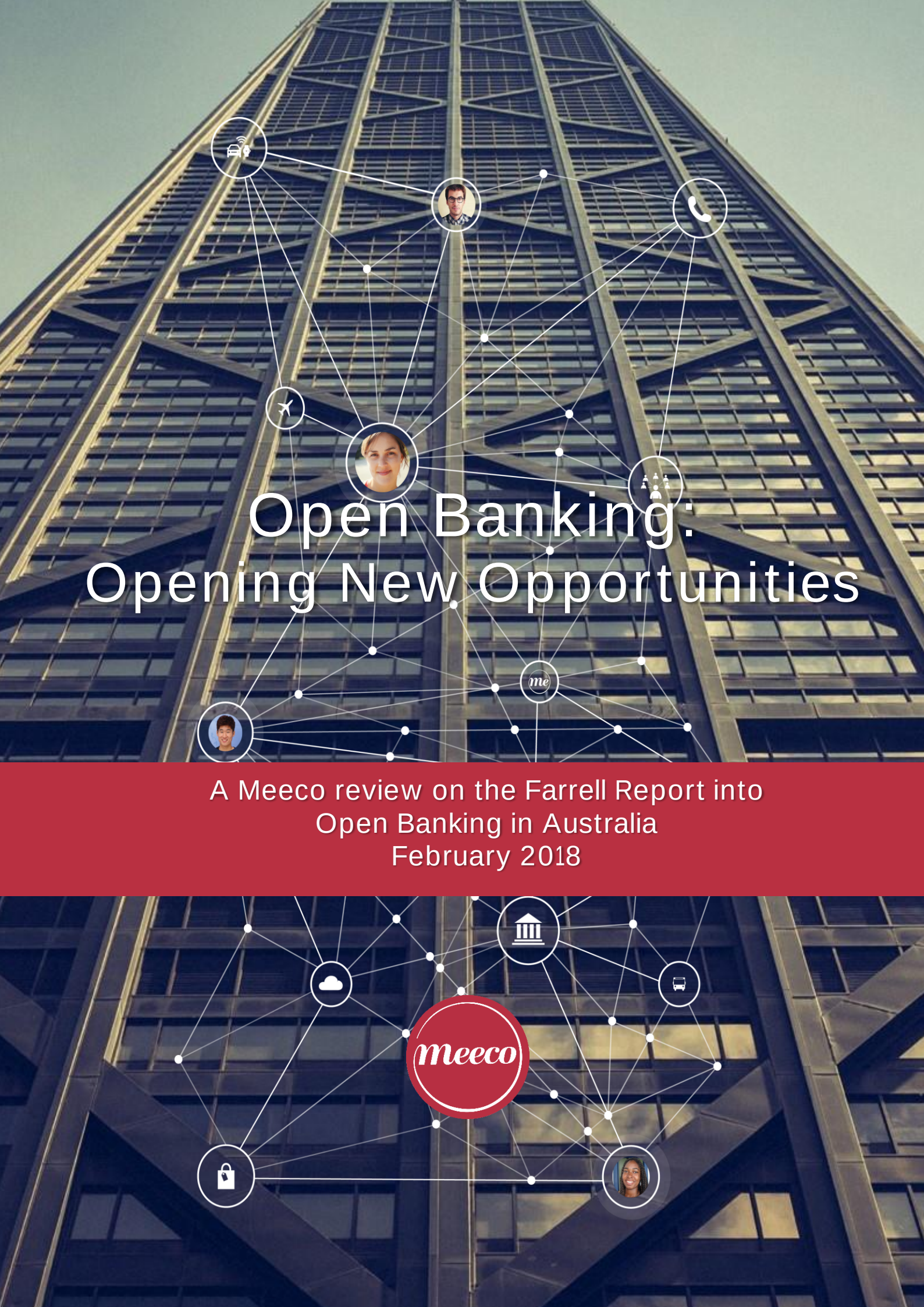


Open Banking: Opening New Opportunities

A Meeco review on the Farrell Report into Open Banking in Australia
February 2018

Key Takeaway

This report provides an overview of some the of key recommendations from the Farrell Report into Open Banking in Australia. It explores how banks can utilise these changes to develop both higher levels of customer trust and introduce new commercial business models.

The Open Banking Review Consultation Period Has Begun

On 9 February, the Australian government published its final Open Banking in Australia Review and launched a consultation period ending 23 March.

This report, which is also referred to as The Farrell Report, is the culmination of the Open Banking Review work Scott Farrell has chaired since July 2017 on behalf of the Hon Scott Morrison MP. Before finalising implementation decisions, the government seeks additional thoughts and recommendations.

Hence, it is important to note that, despite being a final report, this body of work is still a draft.

It is also important to note that whilst Open Banking is the first sector where the national Consumer Data Right (CDR) will apply, the energy and telecommunications sectors will soon follow. The final regulatory framework here will shape and influence those and all other subsequent sectors.

What Publications and Tools Has the Government Made Available?

The Treasury has created several useful links to facilitate reading, understanding and responding to the Farrell Report.

1. Open Banking in Australia Review

- This is the full report comprised of six chapters addressing context, regulatory framework, scope, safeguards, data transfer and implementation.
- The foreword speaks to the purpose of Open Banking (*champion customer data rights; increase customer choice via competition and new products and services; implement efficient, fair, sustainable practices with security and privacy top of mind*) and how open banking could positively influence the future (*a customer-centric data sector and a broader data ecosystem should lead to growth, employment, expertise and value*).

- The executive summary succinctly describes each of the six chapters and each of the fifty recommendations. If nothing else, read and distribute these twelve pages to colleagues and teams.
- A period of approximately 12 months between the announcement of a final Government decision on Open Banking and the Commencement Date should be allowed for implementation. This is viewed as an aggressive timeline.
- The report ends with a useful glossary, key acronyms and a detail-rich appendix.

2. Consumer Data Right (CDR) Fact Sheet

- Explains the relationship between CDR and Open Banking
- Provides a history and overview of CDR including next steps
- Shares benefits and a few customer use case examples
- Calls out the areas where it is looking for industry input
- Presents current regulatory thinking and future sectors designation

3. Consultation website

- Contains the above documents
- Instructs how to respond to the consultation

“The hallmark of a future-proof organisation will be the willingness to share the data it collects about its customers directly with its customers for mutual value”

Katryna Dow, Meeco

Why Open Banking Will Benefit Both Banks and Customers

A key takeaway is that banks and financial institutions can leverage Open Banking to develop higher levels of customer trust and introduce new commercial business models based on that earned trust.

By giving customers greater access to and control over their banking data and digital assets, Open Banking has the potential to transform the way in which customers use and benefit from the banking system. Consent and permission mechanisms give customers a greater say in who uses their data, how and when. This includes third-party exchanges.

This is a marketing nightmare and a compliance tick-the-box exercise, right? No, there is a silver lining. Treating customers' personal data, identities and digital attributes more transparently and respectfully opens doors to new customer opportunities and relationships based on trust, accuracy and privacy by design.

Customers are weary and wary. Thanks to rampant data breaches and global internet giants' bad behaviours and practices, customer expectations regarding how enterprises manage (or mismanage) their data are changing. Customers are increasingly more informed and educated about the collection and use of their personal digital information.

By embracing Open Banking and approaching it as a viable commercial model, banks can introduce new levels of customer engagement and develop deeper trust.

Where Should a Bank or Financial Institution Start?

Start by recognising Open Banking is coming and start treating customer trust as a Board level strategy. Three Farrell Report recommendations to prioritise now are:

1. Customer Control (Recommendation 4.5)
2. Persistent Authorisation (Recommendation 5.6)
3. Intermediaries (Recommendation 5.8) and A new data ecosystem to advance the digital economy (Chapter 6: Implementation and beyond)

Each of these recommendations will develop deeper customer trust and introduce new levels of engagement.

Recommendation 4.5: Customer Control

A customer's consent under Open Banking must be explicit, fully informed and able to be permitted or constrained according to the customer's instructions

(Farrell Report Pages xvi and 60-61)

Customer Control (Recommendation 4.5)

Consent is at the very heart of every customer data right. Customer consent is at the heart of any open data ecosystem.

The currently proposed regulation will require banks and financial institutions to gather new forms of customer consent when collecting and processing personal information. Customers will have more control as to how their data is used, by whom and for what purpose.

Requirements call for requesting and receiving more transparent consent. The consent will need to be clearly related to the context of the data exchange process, what the report calls 'specific as to the purpose' (when requested by a data recipient).

Undoubtedly, this change will impact existing digital marketing programs and likely enterprise-wide customer relationship management (CRM) use as well.

Forward-thinking organisations should view giving customers greater control over their data as a smart business strategy. Why? A 'give-to-get' approach strikes a thoughtful balance between data control, consent and trust.

Evidence from recent Meeco consent trials in Europe indicates that customers with more ownership over their personal data tend to keep it more accurate and up to date. That is very helpful and cost-efficient for a bank or financial institution because it provides a more accurate and contextual customer understanding when the customer exchanges data as part of a digital journey. There isn't any aggregated, anonymised data to unravel and no finger crossing needed regarding accuracy or authenticity.

Obtaining these small contextual data sets with permission produces a true "segment-of-one" and enables new levels of personalisation. Thus, contextual consent can lead to the holy grail for many marketing teams.

Recommendation 5.6: Customer Control

Customers should be able to grant persistent authorisation. They should also be able to limit the authorisation period at their discretion, revoke authorisation through the third-party service or via the data holder and be notified periodically they are still sharing their information. All authorisations should expire after a set period.

(Farrell Report, pages xvii and 88-89)

Persistent Authorisation (Recommendation 5.6)

The average customer manages up to thirty digital relationships at any one time. Thus, there could be potential cognitive overload associated with giving, controlling and changing consent and permissions. Customers will need a way to easily manage what could become a complicated issue. Finding a practical, customer-centric solution to avoid consent fatigue will require thought, testing and iteration.

The type of data and contextual nature of why the data is being exchanged are equally important considerations when designing systems and new customer experiences. This is particularly relevant to banking and financial decisions.

The emergence of separate, individual bank authorisation and consent mechanisms should be avoided. Not only would this be an administrative nightmare, it would also stifle uptake and use by customers for all parties. Everyone loses: customers, banks, financial institutions, participating third-parties, the economy.

Meeco enables the most customer friendly option: a centralised, easy to view "permissions and consent dashboard" integrating all digital relationships. A single place to review, revoke and edit permissions. To implement a unified layer such as this, banks and financial institutions would need to collaborate or engage intermediaries.

Given that banks and financial institutions are already using intermediary tokens with emerging and established authorisation and verification protocols such as OAuth 2.0, it's not a far stretch to imagine them used here for Open Banking as well.

The lead up to the European General Data Protection Regulation (GDPR), which goes into effect May 2018, has shown that consent and permissions are some of the most complicated areas to get right. Consent means different things to different people as does the access level granted to specific data sets for specific outcomes. Whilst it is still early days, Australian banks are at an advantage by learning from European examples as these new regulations are implemented.

Recommendation 5.8 – intermediaries

The Standards should allow for delegation of access to intermediaries such as middleware providers

(Farrell Report, pages xvii, 90-91)

As the connections increase and participants come to rely on the customer-directed flow of data between them, a data ecosystem should emerge. The increasing use of data, in a secure ecosystem with a strong governance structure, could be tremendously beneficial.

From a customer perspective, the ability to provide their data that is held by one service provider (like a bank) to another in a completely different sector (like a telecommunications provider) could enable an entirely new field of products and services to be offered, enhancing choice and convenience. For data holders and recipients, this new potential source of information enables better services to be offered, and a more precise product design to meet customer needs.

The more successful the ecosystem is, the more the participants will grow to rely on it.

(Farrell Report, 111-112)

Intermediaries (Recommendation 5.8) and A new data ecosystem to advance the digital economy (Chapter 6: Implementation and beyond)

The Consumer Data Right's promise of a wider scope across other verticals in the near future highlights the biggest business opportunity: a truly open data landscape where individuals and businesses can exchange and re-use data across different digital relationships. Forward-thinking businesses in Europe are already tackling this and benefiting from testing and iterating.

A new data ecosystem requires intermediaries and includes customers who do not use online banking but may still wish to authorise digital data exchanges with third-parties.

Most customer data lives in corporate silos and CRMs. Not only is it currently extremely difficult, if not impossible, for the individual to re-use their data in more than one of these environments, the same holds true for many banks and financial institutions who are unable to share data across different divisions or service lines within the same institution.

A new data ecosystem where customers can efficiently and directly exchange consent-based data with multiple service providers has the potential to transform existing business models, reduce operational costs and enable new forms of customer engagement such as personalisation to emerge.

Intermediaries like Meeco may provide the answer and unlock new value. The introduction of a common, API-driven, horizontal customer layer could simplify bringing these data ecosystems to life. Think of it as a consent-driven attribute exchange or service orchestration layer connecting and protecting all participants (entities, data and services).

To bring this ecosystem to life, think about a scenario such as opening a bank account or applying for a credit card. Customers must submit substantial personal information and identity documentation. Currently, there isn't an easy way for customers to capture their data and re-use it with trusted third-parties.

As a result, Know Your Customer (KYC) processes retain significant levels of friction and remain costly. Customer drop-off rates remain high as does customer frustration due to the need to repeatedly submit similar information to multiple third-parties, let alone to the bank they might've already done business with.

If data such as identity and verified claims could be securely accessed and re-purposed, this would create new business models. This service would effectively

provide the customer with a 'remote control' to collate and re-use their data with consent and permission for new and improved outcomes.

Could existing trusted enterprises like banks and financial service providers facilitate such a life management service and become network operators in new personal data ecosystems? Or, should this be provided by independent third-parties?

If the bank or financial institution could offer the customer a secure place to store tokenised KYC data alongside other personal data sets, the customer could repeatedly re-use these in multiple digital journeys. This trusted data ecosystem would create new levels of convenience for the customer as well as generate commercial benefits for financial service providers and their partners.

Open Banking opens the door for banks and financial institutions to re-think the data equation and explore new customer engagement-driven business models. This is where financial service providers should focus rather than reducing Open Banking to a compliance and IT exercise.

Meeco, the technology powering consent and personal data

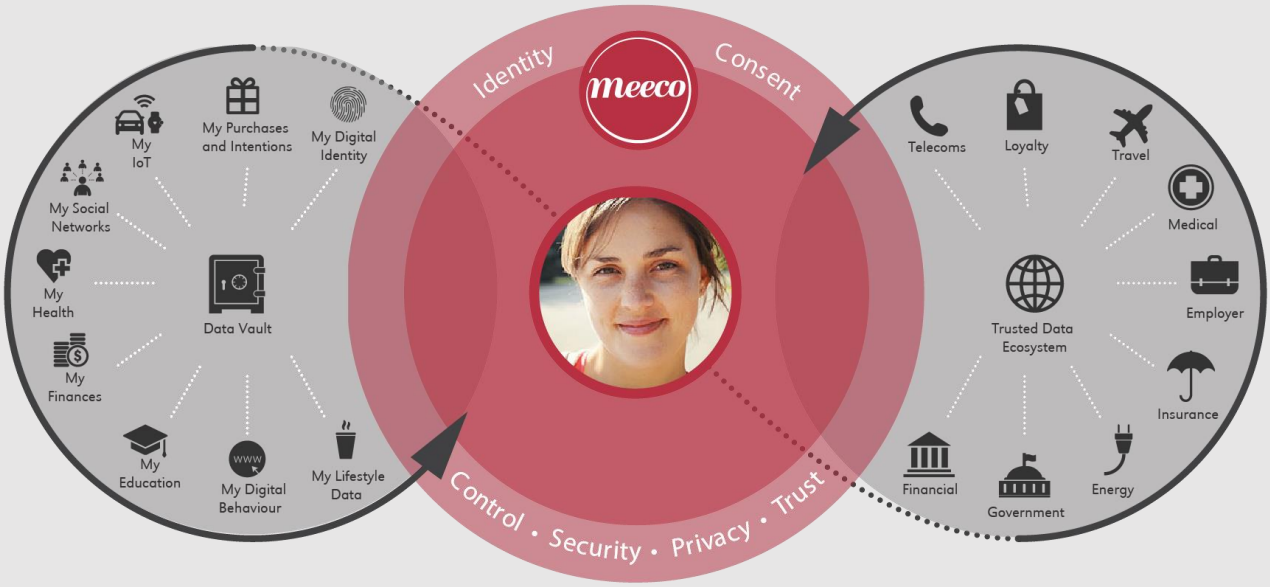
Meeco enables individuals to collate, control and exchange their identity and personal data with the people and organisations they trust. Founded in Australia in 2012, Meeco has been recognised as a global innovator and leader in the emerging personal data economy. Now with offices in the UK and Europe, Meeco is working at the forefront of the changing personal data regulation and Open Banking.

For enterprises, Meeco enables trusted data ecosystems and new business models to be developed in partnership with customers. Meeco's API-of-Me provides customers with the ability to aggregate personal data across their life including identity, social, IoT, finance, health and lifestyle, and share it directly as part of a digital value chain.

The Meeco platform includes:

- A suite of APIs
- A Consent Engine
- Immutable digital timeline of real-time, accurate personal data
- iOS, Android and Web Attribute Wallet
- Privacy by Design tools to support privacy compliance and audit

The Meeco Personal Data Ecosystem



The Meeco platform with personal attribute wallet and trusted ecosystem of service providers

Powered by Meeco, customers are able to share context and intent in exchange for personalised products and services. This rich small data provides a true segment-of-one view.

How Meeco Can Assist Now?

Meeco, a certified Microsoft partner has developed an Open Banking Sandbox for enterprises to test hypotheses and prove business value prior to making substantial investments.

The Open Banking Sandbox is a custom designed, flexible process and pathway to new products, services, experiences and business models. Several leading European financial institutions have already utilised it to build and test compliant, viable open data innovations, generating new value streams for all parties.

Meeco is well equipped to help enterprises navigate through both the emerging personal data landscape and the benefits Open Banking will create for Australian customers, financial service providers and the wider economy.

The Meeco platform not only addresses emerging personal data regulation but also empowers enterprises such as financial service providers to participate in the new commercial opportunities presented by Open Banking and the open data economy.

Meeco is well positioned to understand and work closely with Australian banks and financial service providers as they enter this new era of personal data control.

Our global partnership with Microsoft enables secure and scalable costumer identity and access management solutions to be integrated into new consent-based data journeys.

As members of the Kantara Initiative we are helping to pioneer new interoperability frameworks for personal data exchange through their User Managed Access (UMA) protocol.

Active member of FinTech Australia and a contributor to working group policy discussions around Open Data.

A resident of Stone and Chalk in the new Sydney Start-up Hub, the largest fintech hub in the southern hemisphere.

Meeco is listed in the One World Identity Landscape in the Personal Identity category.

Meeco's Founder and CEO, Katryna Dow is recognised as one of the top global identity influencers in 2018.

For more information, please visit www.meeco.me or contact us directly:

Mike Page
Head of Platform Partnerships
Australasia
mike.page@meeco.me

Elizabeth Boerner
COO
UK/Europe
elizabeth.boerner@meeco.me

Katryna Dow
CEO and Founder
Global
katryna.dow@meeco.me