Review into Open Banking Australia

WSO2 Submission

Date: 23rd March 2018

WSO2 Australia Ltd., 9 Castlereagh Street, Sydney NSW 2000, Australia
Tel: +61 2 8249 1888 | **Email:** bizdev@wso2.com

Cover Letter

Open Banking Review Secretariat
The Treasury
Langton Crescent
PARKES ACT 2600

Dear Mr. Farrell,

WSO2 Inc. is pleased to submit its response to the Review into Open Banking Australia, based on our experience of providing technology for PSD2 Compliance and Open Banking in Europe and UK.

We commend the Australian government and the Review committee for putting in place a judicious and farsighted open data strategy by way of the Consumer Data Right and Open Banking, which in our opinion paves the way for a significant change in Australian citizens' lifestyles in the future.

We are proud of the impact we have made in helping various banks ranging from small to medium enterprises to large multinationals who provide Open Banking facilities to their customers.

Our response is a combination of our analysis of the Australian Open Banking requirement and strategy, and our experiences as members of the OBIE Working Group and our involvement in providing input to Standards such as the Berlin Group.

We hope our response would be useful in shaping the Australian Open Banking strategy, especially from a technology perspective.

For inquiries regarding this response or any other related matter, please contact me through the following contact information:

Correspondent Details	
Name	Seshika Fernando
Designation	Head of Financial Solutions
Email	seshika@wso2.com

Thank You,

Seshika Fernando

Table of Contents

1. Introduction

The Australian Government seeks consultations on the Review into Open Banking in Australia. This will be the first phase of the Australian Consumer Data Right which provides consumers with rights to direct that a business transfer data on the consumer, to a third party, in a usable machine readable form.

This document is WSO2's official response to the Review into Open Banking in Australia and is organized as follows.

- **About WSO2:** This section introduces the strengths of WSO2 as a vendor and its expertise in the open banking space. provides an introduction to WSO2 and
- **Open Banking Implementation Considerations:** This section discusses the areas to be considered when implementing open banking in Australia in terms of connectivity, authentication and authorization, data requirements, and implementation.
- **Open Data - The Game Changer:** This section presents ideas around the possible opportunities of the new ecosystem created through the implementation of Open Banking and the Consumer Data Right
- **Technology for an Open Data Ecosystem:** This section describes the technology capabilities that enterprises will require in order to thrive within this new open data ecosystem.

2. About WSO2

WSO2 is an open source company that provides the technology enablers for digital transformation. It is best known for its integration, API management, identity and access management, and analytics offerings, some of which are notably used by eBay, Bank of New York Mellon, and Experian.

Today, enterprises need to leverage technology to transform customer, partner, and stakeholder experiences as well as internal operations in order to become an agile, competitive business. WSO2 simplifies the core problems of enterprises undergoing digital transformation with its highly scalable and innovative product suite. The WSO2 platform has been instrumental in delivering technology excellence to global customers[1] across several industries such as banking and finance, healthcare, retail, education, government, and manufacturing. WSO2 works with an extensive network of partners[2] to deliver these implementations.

2.1. WSO2 Open Banking

WSO2 Open Banking leverages the WSO2 Platform to provide a complete technology stack to support a customized and accelerated technology experience for Open Banking. It comes with:

- Financial APIs with secured invocation
- Ready to use API templates for popular Open Banking API Standards
- Strong customer authentication
- User consent management
- Third-Party Provider (TPP) onboarding capabilities
- Integration points for core banking systems and external services
- API Analytics and Dashboards

The strength of the WSO2 Open Banking solution and domain expertise of the development and services teams have helped top European banks comply with PSD2 within aggressive timelines. WSO2 is committed to contribute to the technology development within open banking and are keen to take our learnings from Europe and UK to the rest of the world.

[1] https://wso2.com/about/customers/
[2] https://wso2.com/partners/

3. Open Banking Implementation Considerations

Even though Open Banking is not new and has been adopted by other regions in the world, the Australian implementation is unique in many ways. This section highlights some of the concepts that are unique in the Australian context and discusses key considerations and options available to tackle each area.

3.1. Connecting Data Recipients with Data Holders

Accreditation Validation

The dynamics of the onboarding process has to be thought through in great detail. This is especially important in order to avoid some of the confusions that have arisen among the banking networks in Europe regarding the expectations of onboarding TPPs on to Banks' Open Banking platforms.

For consumers to be able to instruct their data holders to share data with chosen data recipient(s), the data recipients need to be onboard to the data holder's API platform. The first step in achieving this is for data holders to provide a registration process whereby data recipients' accreditation is verified, and then allow access to APIs that are relevant to the accreditation tier of the data holder.

The first concern, therefore, is how data holders will perform the accreditation verification. The Review report mentions a central address book, which participants and customers can use to validate the accreditation of any participant. This address book needs to be available in an electronic format, which enables data holders to programmatically validate the accreditation of a participant that sends a registration request to the data holder. One way to do this is using a digital certificate, which contains information about the accreditation tier of the participant. Once the accreditation tier is confirmed, the data holder can provide the data recipient with access to the APIs that are relevant to the specific accreditation tier.

One of the accreditation criteria should be that the data recipient is able to transfer data to other data recipients. This is to ensure that all data recipients are able to comply with a customer's direction to share data with other participants.

Sandbox/Production Environments

Once the data recipient is onboard to the data holder's API platform, the data recipient should be provided with a sandbox environment that provides the documentation on how to subscribe to and consume the APIs visible to the data recipient, in order for the data recipient to connect their data receiving application with the APIs and test the process flow.

Once the data recipient is satisfied with the ability to consume the APIs successfully, they can request the data holder to provide them with the access to the production environment, where the data recipient can start receiving data as directed by the consumers of the data holder.

Accreditation Upgrades, Downgrades, and Revocation

The accreditation tier that is provided to a data recipient can change in the future. There can be three types of changes.

1. The need to upgrade the accreditation of a data recipient based on a change of circumstances that allow them to qualify to receive higher-risk data.
2. The need to downgrade the accreditation of a data recipient based on a change of circumstances that disallow them to receive higher-risk data that they were previously privy to.
3. The need to revoke the accreditation completely due to a change of circumstances such as severe security vulnerabilities that leave the data recipient unfit to handle customer data.

When the accreditation status of a data recipient changes in the above ways, there should be a mechanism by which, data holders are automatically and immediately notified in order for them to make the necessary changes to the API subscriptions of the data recipient(s) in question. A push notification mechanism from the central address book to the data holders would be desirable, in order to enable the data holders to share data based on up to date accreditation information.

Incident Reporting

A mechanism for all the participants to report incidents to the regulator is required. Data holders will need the ability to report violations or abuse of their API platform by accredited data recipients. Data recipients will need the ability to report unavailability or connectivity issues of the data holder's API platform. Each of these notifications should initiate a re-evaluation of the relevant

participants' conformance to rules and/or standards and therefore impact their accreditation status and/or result in fines/penalties. Temporary suspension mechanisms should also be in place, in order to allow the regulator to investigate an incident and take action to either dismiss the claim and lift the suspension or downgrade or revoke the accreditation of the participants who have violated the rules.

3.2. Authentication and Authorization

There are many ways for customers to provide data transfer instructions to the data holder. The relevant authentication and authorization process for each option will be different and therefore needs to be addressed separately.

Consent via Data Holder's Application

When a customer's request to share data is sent to the data holder through the data recipient's application, the data holder needs to employ a direct channel with the customer. This enables to independently authenticate the user and obtain customer authorization for the desired data transfer.

The Review report recommends a redirect model for authentication as a starting point and mentions that Multi-Factor Authentication (MFA) is a possible option to mitigate risks of phishing and other attacks, even though MFA may impact the customer experience. However, as the request to transfer data is typically a one-time instruction and as the authorization will be persistent in most cases, necessitating MFA within a redirected authentication mechanism is not unreasonable as this can minimize phishing and other attacks to a great extent. The typical steps involved would be as follows.

1. A customer accesses the aggregator application in order to add a bank account to it
2. The aggregator application redirects the customer to the bank's authentication page that is accessed via the bank's authentication API.
3. The bank performs MFA with the customer.
4. The bank displays a page through which the customer specifies the datasets the bank should share.

5. The bank grants an authorization code to the aggregator application on behalf of the customer.

6. The aggregator application exchanges this authorization code with an access token by directly calling the bank's token endpoint.

7. The aggregator application uses the access token (until its expiry date) to access the customer's data in the future.

Note: When the data recipient is a mobile application, it is advisable to make use of Proof Key for Code Exchange (PKCE), to mitigate the risk of authorization codes being stolen by malicious applications installed in the mobile.

Physical or Written Consent

The customers who do not have the online banking facility require an alternate method of providing authorization for data transfer. The customers could typically provide instructions in written form or by visiting a bank branch and informing a bank teller. In each case, an employee of the bank will need to capture the customer's consent instruction and enter it to the bank's IT system. It would be prudent to require the bank to capture the following information along with the customer authorization.

1. How the consent was communicated, i.e., physically visiting branch, by letter, power of attorney, etc.

2. When the consent instructions were received and added to the system.

3. Who entered the consent instructions to the system.

The above information will be important for future dispute resolutions as the customer consent was not directly entered to the bank's system by the customer.

While instructing one-time data transfer via this method is possible, maintaining persistent consent through a physical or written mechanism may be impractical. This is because persistent consent always has an expiry date, and needs to be renewed by the customer periodically.

Business Customers

Corporate accounts involve multiple users with different authorizations where some can only view transactions, some can execute transactions up to a limit, some transactions need the authorization of a complex pattern, e.g., 2 out of 3 directors, etc. Therefore, the authorization for data transfer relating to corporate accounts will be much more complicated than that of joint accounts. These combinations and permutations will have to be individually addressed when capturing the consents as well as managing the notifications regarding the data transfers and handling the terminations of data sharing arrangements initiated by other users.

3.3. Data

Security Requirements for Transaction Data and Product Data

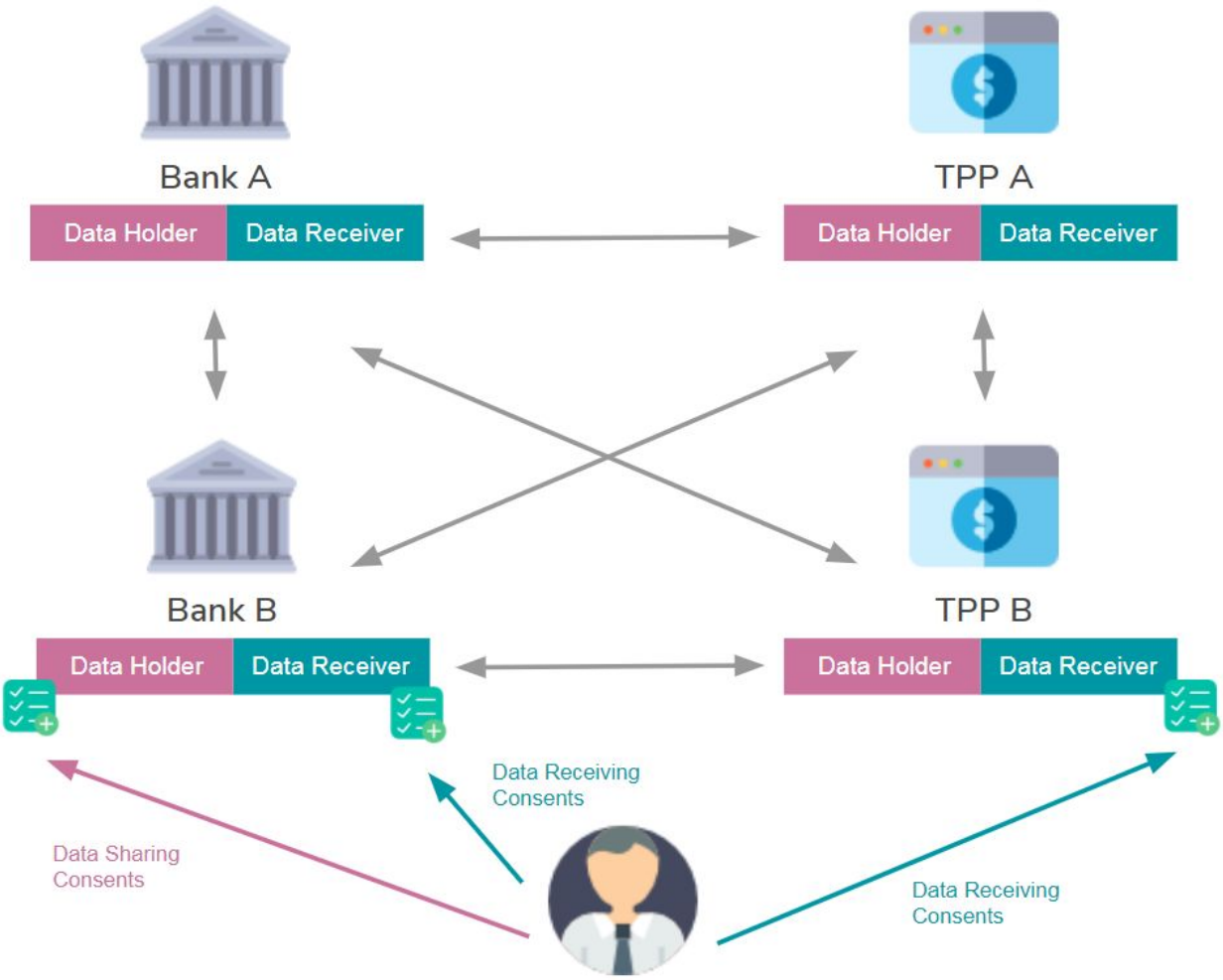
While the transfer of customer transaction data will require the customer's explicit consent, product data should be an open API that does not require customer consent.

Aggregate Information on Transferred Data

As explained in section 4.1 of this document, there is a significant value that can be created by sharing aggregate (and therefore anonymized) insights gained through transaction data, to enterprises in other industries (at least until the Consumer Data Right is implemented in other sectors whereby participants in other industries can perform this themselves). Whether the data recipients need to obtain explicit customer consent to use their data for the creation and sharing of aggregate industry insights, need to be considered.

Data Holder and Data Recipient Consent Management

The Review recommends that the Authorized Deposit-taking Institutions (ADIs) be automatically accredited to receive data and that each entity that receives data should be obliged to comply with a customer's direction to share data. This creates a network of entities that are data holders as well as data recipients. Each entity then needs to store and manage, separately, customer consents in the capacity of data holders, i.e., which data should be shared with whom, and of data receivers, i.e., for which purposes the customer's data can be used for.



3.4. Safeguards

The Review provides a comprehensive list of recommendations to ensure a secure Open Banking environment. Another option available to the regulator would be to encourage Open Banking participants to employ anomaly detection mechanisms to identify possible attacks and fraudulent behavior.

Data holders may apply anomaly detection in order to detect irregular API invocation patterns by data recipients, such as abnormal request count, abnormal resource access pattern, unseen source IP access, and abnormal access token renewal.

Data holders may also apply anomaly detection on more behavioral aspects of the customer authorization process such as abnormal consent requests based on customer profile and past patterns.

Data recipients may apply anomaly detection on the data they receive in order to identify any irregularities with regards to message size, message content, etc.

3.5. Developing Technical Standards

According to the Review report, Australia will use the UK Open Banking technical specification as a starting point to create their own technical specification. While the UK Open Banking technical specification is well-written and battle hardened to a great extent by now, the Australian standards should also look to improve the UK specification especially with regards to creating APIs to capture user authorization and catering to the ability to provide fine-grained consents.

3.6. Implementation

As Australia is planning for an aggressive implementation timeline, which tentatively sets aside less than 6 months for technology implementation, it would be useful for the regulator to provide a test suite in order for the ADI's to validate their systems prior to go-live. A test suite provided by the regulator would ensure conformance to standards irrespective of the different technologies employed by different ADI's to implement Open Banking.

It would be in the best interest of each participant to invest in agile and adaptable technology components in order to cater to the future phases not just for Open Banking but the full spectrum of Consumer Data Right in Australia.

4. Open Data - The Game Changer

Open Data ecosystems undoubtedly unlock better experiences and better services for customers. It also opens up new business opportunities and access to new revenue streams to all the participants of the ecosystem. The following is a short commentary of the possibilities and the required technology capabilities to unlock the many strategic benefits of the Open Data ecosystem.

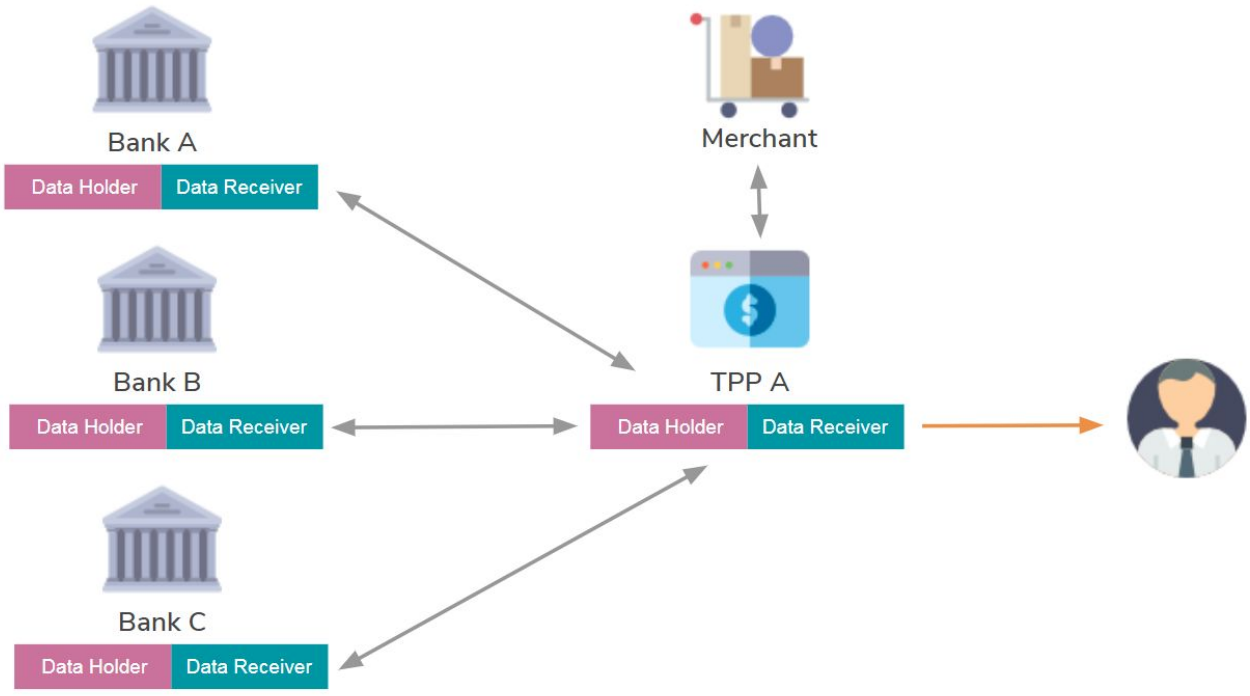
While WSO2 has delivered technology to many European banks to achieve the digital transformation opportunities discussed below, in this section we provide our perspective on the

possibilities uniquely available within the Australian Open Banking environment as well as the implementation of the Consumer Data Right for the broader industry spectrum.

4.1. Market Expansion Opportunities

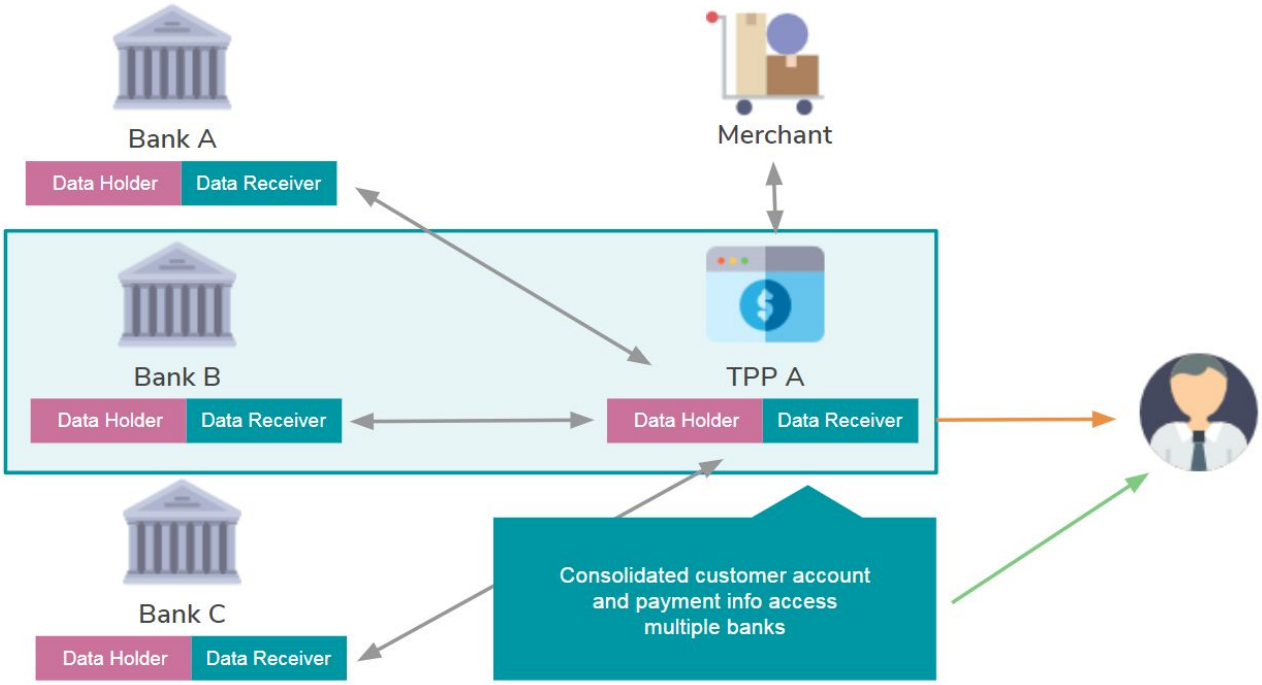
Europe

As the European implementation of Open Banking does not automatically recognize the banks as data recipients, most banks treat PSD2/Open Banking as a compliance requirement with no real benefit to the bank.



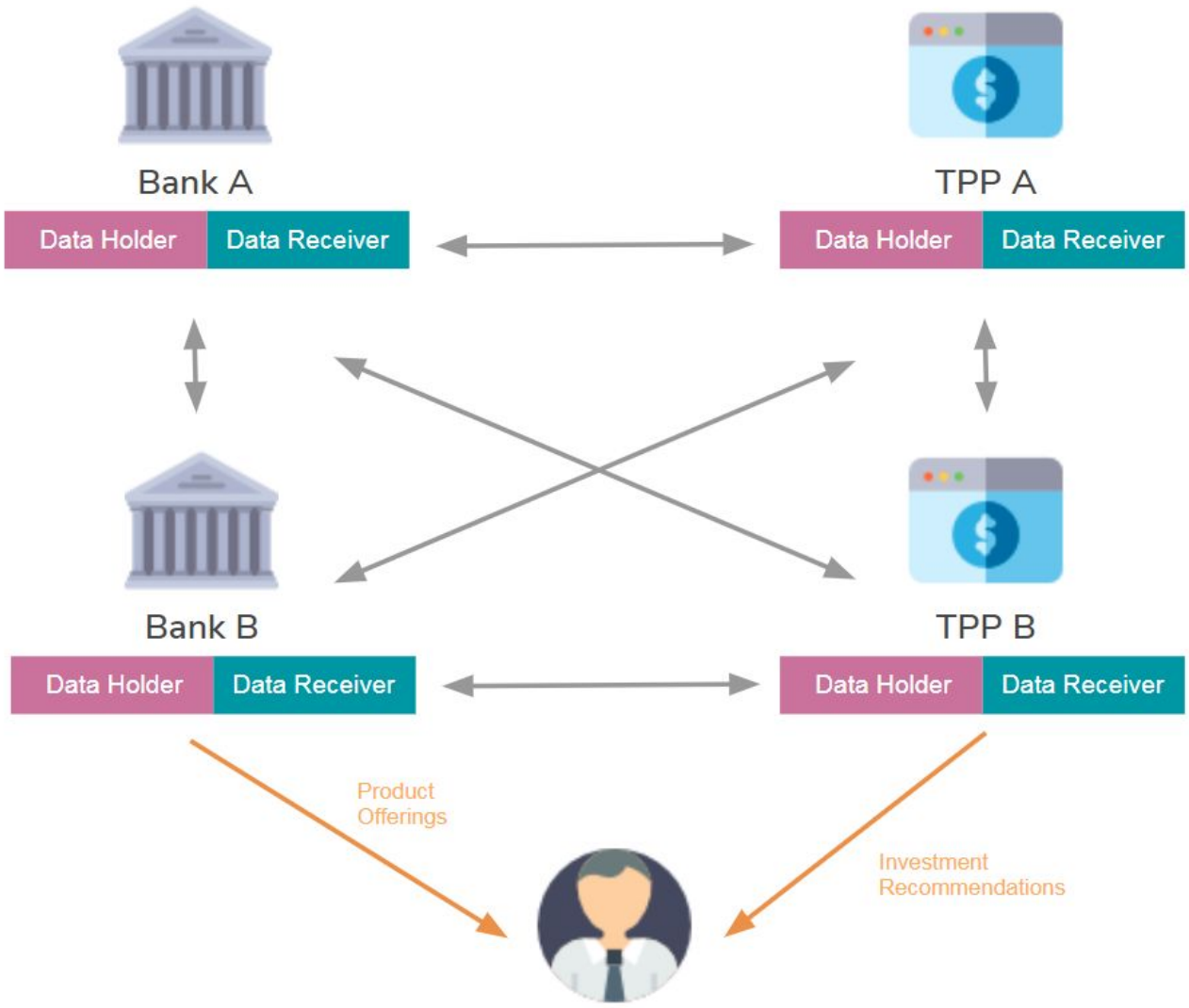
However, the banks that see the opportunities of the Open Banking ecosystem do not stop at compliance. They move on to the next level, where they register themselves as TPPs and are therefore able to consume data exposed by other banks. Banks that offer TPP services gain access to the rich repository of total financial information of customers spread across multiple banks, obtaining a much deeper understanding of its customer base than was possible before. Additionally, such a bank also receives consolidated financial data about its non-customers,

thereby enables gaining valuable insights into market segments that the bank can eventually tap into and expand its portfolio.



Australia

The main advantage in the Australian Open Banking strategy is that all ADIs that are data holders are also automatically accredited to receive data. Under these circumstances, all ADIs automatically have the necessary footing to provide better products and services by gathering more information about the customer's consolidated financial picture, with the customer's consent.



In order for banks to achieve this, they will require technology components that enable them to receive, aggregate, and analyze data in order to create and provide better recommendations and offers to their customers. Banks will need to invest in strong data analytics capabilities in order to thrive, and not just survive in this new ecosystem.

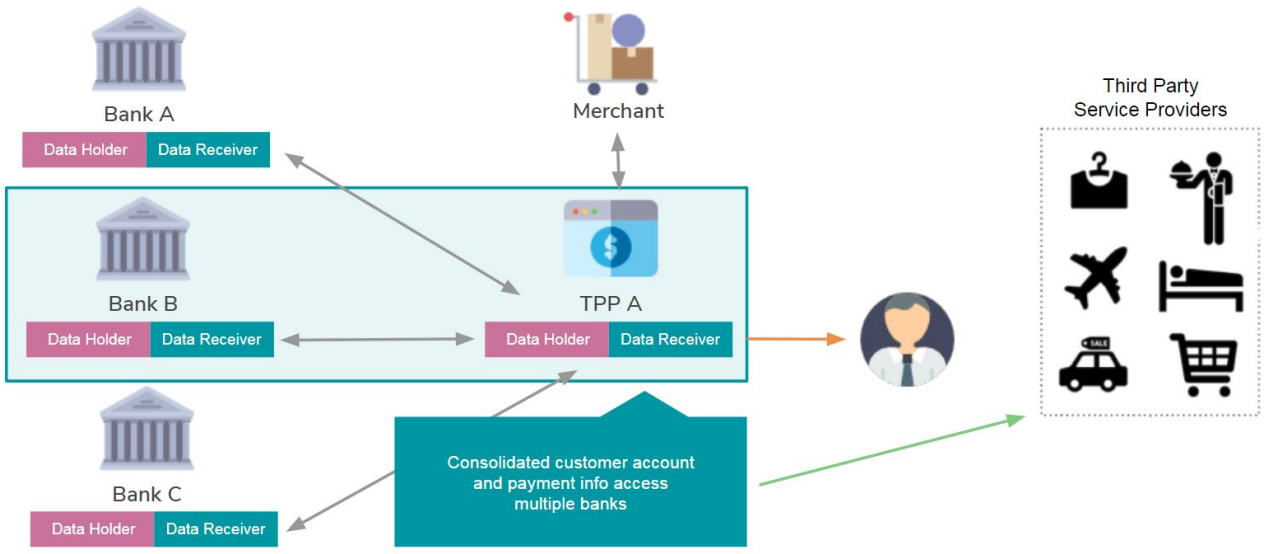
4.2. New Revenue Opportunities

Apart from expanding the business by gaining insights to the bank's customer and non-customer base, the repository of customer financial data enables a bank to provide new products and services that will translate into new revenue streams for the respective bank.

The deep customer knowledge gained through consolidated customer financial information allows banks to analyze and aggregate data and provide business insights that are useful for other industries, such as retail, hospitality, transportation, telecommunication, and healthcare, among others. Banks can provide aggregate insights, such as trends, seasonalities, customer demographics, and even location analytics that help enterprises across different industries to provide contextually relevant products and services to their clientele. This type of insights-based selling adds another new and lucrative revenue stream for the banks.

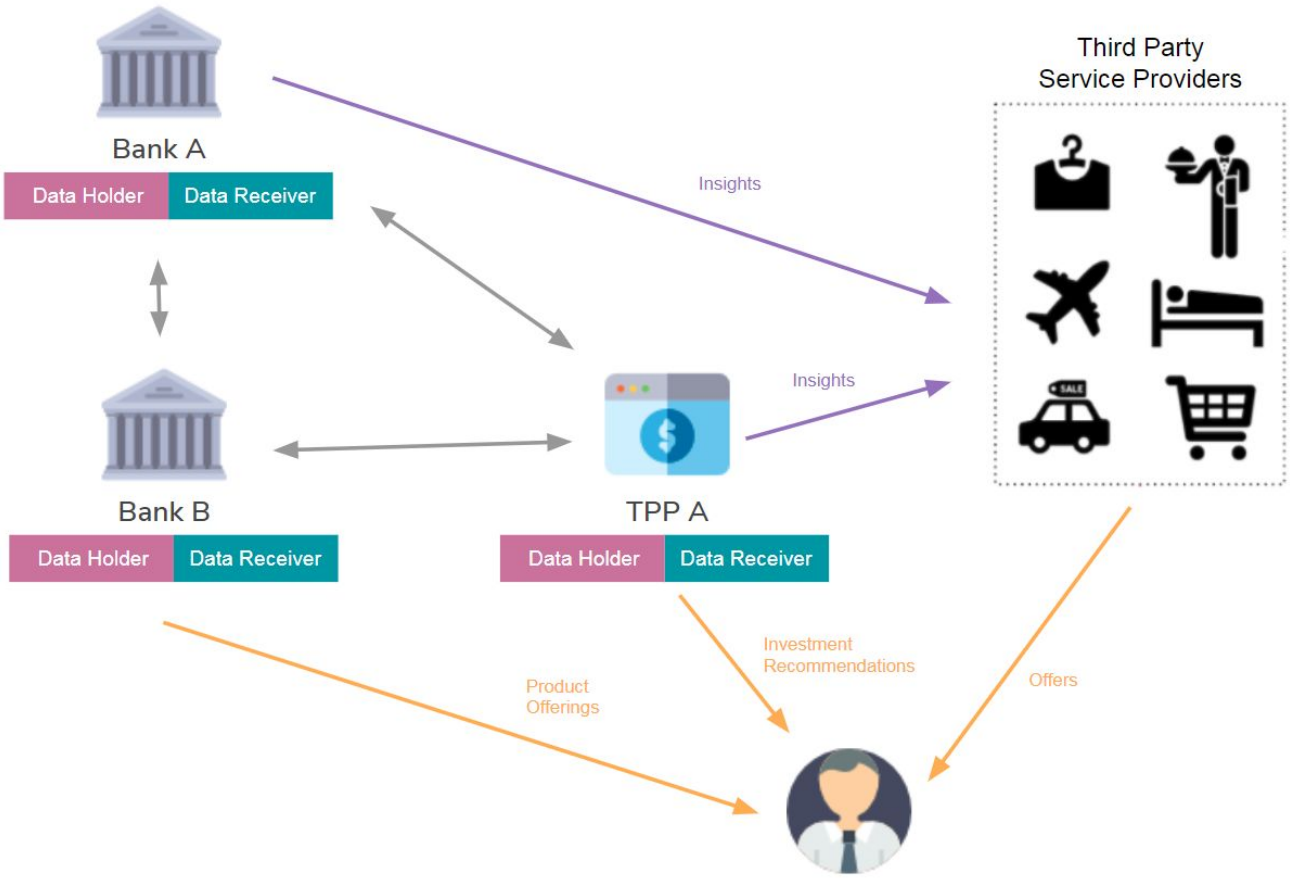
Europe

In the European context, this can be achieved by banks registering themselves as TPPs and then performing analytics on top of the consolidated financial data.



Australia

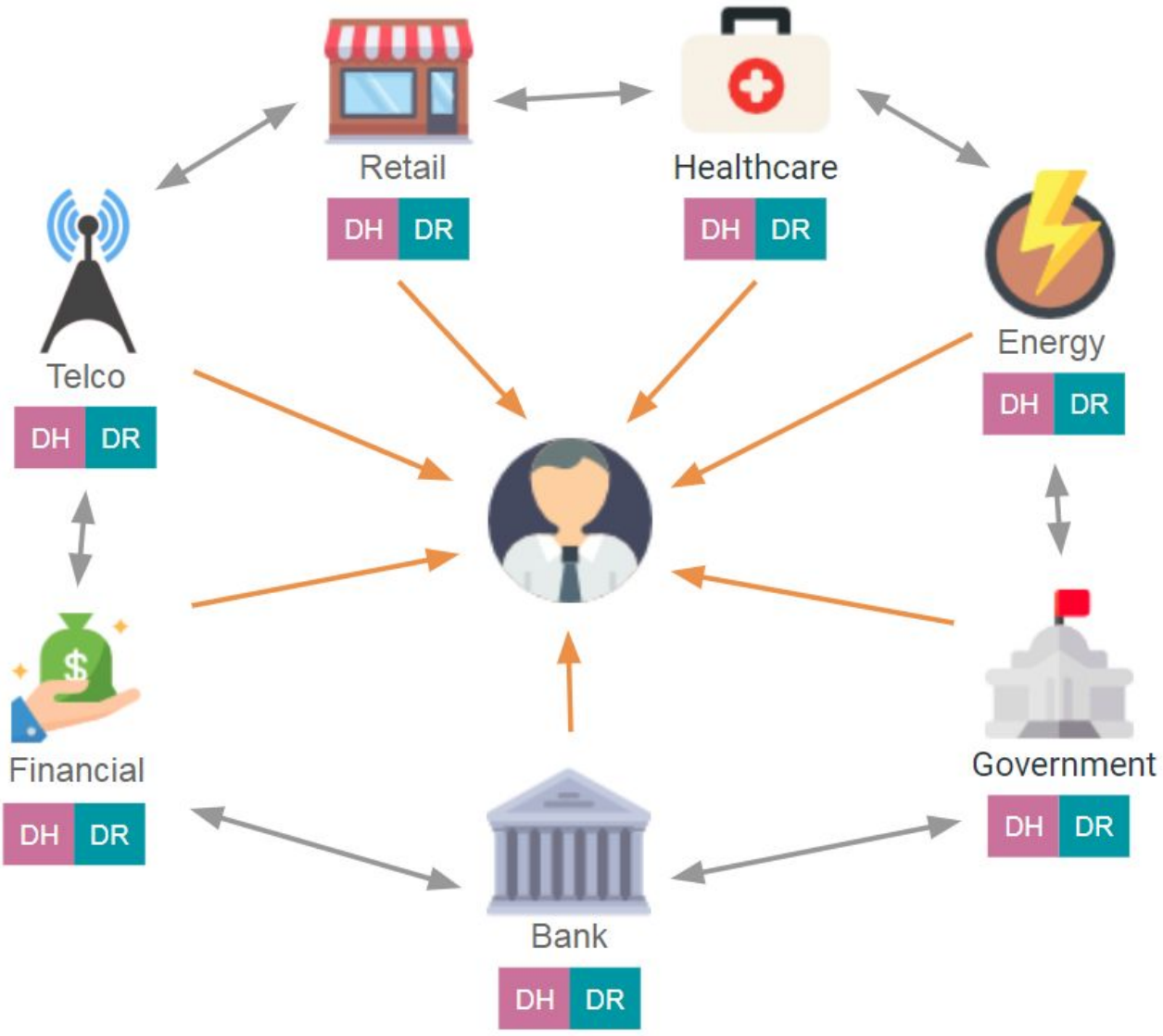
In the Australian context, this opportunity is automatically available to all the participants, as each participant is expected to be a data holder as well as a data receiver.



4.3. Consumer Data Right in Other Sectors

In Australia, Open Banking is only the starting point of a larger open data economy, potentially involving all industry sectors sharing data among each other, with the customer's authorization.

This not only paves the way for a multitude of new digital products and services but also capable of significantly changing the lifestyles of Australian citizens for the better.



Consumers can provide their bank with the authority to make decisions and recommendations for them in many situations. Recommending lending offers based on identifying a flight purchase in order to fund the rest of the holiday or suggesting banking products based on life events are a few examples.

4.4. Considerations for Multi-Sector Write Access

While the Consumer Data Right will be initially based on ‘read’ access only, one of the future considerations would be to enable ‘write’ access. The ‘Write’ access for the banking industry could

mean payment initiation, as is currently available in Europe. It pays however to envision, what 'write' access could mean in the multi-sector open data ecosystem.

One of the possibilities could be the ability for citizens to request service providers, e.g., car dealership, to consume data from their banks and initiate payment for a high-valued transaction, e.g., purchase of a car, by combining funds held at different banks.

Another possibility is for enterprises to piggyback on each other to reach customers within their purchase moments. For example, having searched for a product online, a customer has an offer for that product while on commute en route to a supermarket. The supermarket can reach the consumer's purchase moment and influence his decision by paying the telco to provide an alert to the user about the product on offer, a few minutes before he passes the supermarket.

The above examples are merely scratching the surface of the multitude of opportunities to be gained by this fully integrated open data network where enterprises provide better lifestyle management capabilities to citizens based on the prudent use of their data assets. What is important at this point for all participants of this new world, is not merely to understand the possibilities but also be prepared with the necessary tools such as agile and adaptable technology components that will enable them to innovate and thrive within this brand new data economy.

5. Technology for an Open Data Ecosystem

There is unlimited potential for data sharing within this ecosystem. As stakeholders use data as means of exchange, the technology that sits at the heart of the ecosystem is critical to its success.

While the need for comprehensive technology such as advanced API management, complex integration, extensive identity management, and smart analytics is apparent, the challenge lies in finding a single platform that can deliver it all. The relationships between an enterprise and its technology vendor need to be more strategic.

WSO2 offers a complete technology suite that meets the demands of an open data ecosystem. Our domain and technical experts can work with any type of enterprise and deliver strategic technology direction to thrive in this ecosystem.

6. Glossary

Acronym	Definition
ADI	Authorized Deposit-taking Institution
API	Application Programming Interface
MFA	Multi Factor Authentication
OBIE	Open Banking Implementation Entity (UK)
PKCE	Proof Key for Code Exchange
PSD2	Revised Payment Services Directive
TPP	Third Party Provider