



REVIEW INTO OPEN BANKING CANADA

WSO2 SUBMISSION

Date: 11th February 2019

WSO2 Ltd., 787 Castro Street Mountain View, CA 94041, U.S.A
Tel: +1 650 745 4499 | Email: bizdev@wso2.com

Cover Letter

The Advisory Committee to the Open Banking Review/Financial Institutions Division
The Financial Sector Policy Branch
Department of Finance Canada,
90 Elgin Street, Ottawa, ON K1A 0G5

Dear Advisory Committee Members,

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

We commend the Canadian government and the advisory committee for initiating the first steps in to implementing an Open Banking ecosystem in Canada, which in our opinion paves the way for a significant change in Canadian 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 Canadian Open Banking requirement, and our experiences as members of the OBIE Working Group, NextGenPSD2 Advisory Board as well as Australian Data Standards technical working groups.

We hope our response would be useful in shaping the Canadian 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

| | |
|---|-----------|
| Cover Letter | 2 |
| Table of Contents | 3 |
| Introduction | 4 |
| About WSO2 | 5 |
| WSO2 Open Banking | 5 |
| Open Banking Implementation Considerations | 6 |
| Recommendations on Data Standards | 6 |
| Conformance Certification | 7 |
| Recommendations on Third Party Provider Accreditation and Directory | 7 |
| Recommendations on Security | 9 |
| Authentication Mechanisms | 9 |
| Consent Management | 10 |
| The Scope of Data and Phasing | 11 |
| Open Data - The Game Changer | 12 |
| Expanding the Distribution Channels | 12 |
| Upselling to existing Customer Base | 13 |
| New Revenue Opportunities | 15 |
| Technology for an Open Data Ecosystem | 16 |
| Glossary | 18 |

1. Introduction

The Canadian Department of Finance seeks consultations on the Review into the merits of Open Banking in Canada as part of a two-phased approach to understanding the Canadian requirement for Open Banking and choosing the relevant implementation options.

This document is WSO2's official response to the Review into the merits of Open Banking in Canada 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.
- **Open Banking Implementation Considerations:** This section discusses the areas to be considered when implementing Open Banking in Canada in terms of connectivity, security, 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.
- **Technology for an Open Data Ecosystem:** This section describes the technology capabilities that banks will require in order to thrive within this new open data ecosystem.

2. About WSO2

WSO2 is the world's #1 open source integration vendor, helping digital-driven organizations become integration agile. Customers choose us for our broad integrated platform, approach to open source, and agile transformation methodology. The company's hybrid platform for developing, reusing, running and managing integrations prevents lock-in through open source software that runs on-premises or in the cloud. Today, hundreds of leading brands and thousands of global projects execute 6 trillion transactions annually using WSO2 integration technologies. Visit <https://wso2.com> to learn more.

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
- Transaction Risk Analysis (TRA) and fraud detection
- 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 contributing to the technology development within Open Banking and are keen to take our learnings from Europe, UK, and Australia to the rest of the world.

3. Open Banking Implementation Considerations

Even though Open Banking is not new and has been adopted by other regions in the world, each country's Open Banking requirements and scope is unique. This section highlights some key concepts that should be considered for the Canadian Open Banking regime.

3.1. Recommendations on Data Standards

WSO2 strongly recommends the Canadian Open Banking Regulator to create a Data Standards Body which can create technical standards not just on APIs but also security as well as reporting requirements. The availability of a single standard is essential for the optimal performance of the Open Banking ecosystem, which provides a standard method for Third Party Providers to consume Open Banking APIs.

In developing technical standards for Open Banking in Canada, our recommendation is to use the Open Banking UK specification as a base and localize the standards to cater to specific Canadian requirements. The Open Banking UK specification is one of the most matured Open Banking technical specifications currently available, owing to the multiple revisions it has gone through as a result of feedback provided by British Banks (especially CMA order) implementing the standards. The Australian technical standards have also followed the same practice and it has helped them to really focus on the localization tasks in order to make the standards work well for Australia, rather than spending time and effort on creating a standard from scratch, a task that has already been undertaken and completed by the British regulator.

This will also result in maintaining a general commonality between standards across the globe allowing Account Aggregation Providers and Payment Service Providers who operate globally, to provide services to customers who have bank accounts distributed across different regions of the world. It also simplifies the technology implementation for subsidiaries of foreign banks and foreign banks doing business in Canada (which account for more than 50% of the banking industry in Canada) considering the technology evaluations and procurement cycles that have already taken place for similar Open Banking projects in UK, Europe or Australia.

3.2. Conformance Certification

It would be useful for the regulator to provide a test suite in order for the Banks to validate their systems prior to go-live, and obtain a conformance certification. A test suite provided by the regulator would ensure conformance to standards irrespective of the different technologies employed by different Banks to implement Open Banking.

3.3. Recommendations on Third Party Provider Accreditation and Directory

One of the critical success factors of a well functioning Open Banking ecosystem is a sound Third Party Service Provider accreditation facility as well as a digitally accessible directory that can be used to validate the Third Party Providers and their accreditation levels. This section details some important considerations in creating a secure and fair-for-all Open Banking regime.

Accreditation

WSO2 recommends the Canadian Department of Finance to consider setting up or appointing an existing organization to perform due diligence on each Third Party Financial Service Provider and awarding a certificate of accreditation prior to allowing them to gain access to Open Banking API portals of banks. This is essential in order to both protect the banking systems and infrastructure as well as customers who can be potentially hoodwinked by undesirable Third Party Providers in order to gain access to their financial data.

This accreditation program can be conducted either as a single accreditation or a tiered accreditation based on certain criteria that allow different levels of data access based on the financial and technological stability of the Third Party Provider organization. The need for a tiered accreditation program would largely depend on the scope of data that are to be exposed as APIs and whether the datasets vary in sensitivity and importance to the customers.

Directory

Once the accreditation process is in place, the Open Banking ecosystem will require a digitally accessible directory that lists out the accredited Third Party Providers along with their accreditation tiers (if any). This Directory will be programmatically accessed by each Bank's Open Banking API

portal in order to validate requests by Third Party Providers, prior to allowing them access to the secured APIs.

This Directory can also be used to provide a listing of all Banks that are Open Banking compliant along with links to their Open Banking API portals, which will enable Accredited Third Party Providers to easily discover all API portals that they can integrate their applications with.

Sandbox/Production Environments

Once the Third Party Provider is on-boarded to the Bank's API platform, the TPP should be provided with a sandbox environment that provides the documentation on how to subscribe to and consume the APIs visible to them, in order to connect their application with the APIs and test the process flow.

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

Accreditation Upgrades, Downgrades, and Revocation

If a tiered accreditation program is followed, the accreditation tier of a Third Party Provider can change in the future. There can be three types of changes.

1. The need to upgrade the accreditation based on a change of circumstances that allow them to qualify to receive higher-risk data.
2. The need to downgrade the accreditation 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 Third Party Provider unfit to handle customer data.

When such an accreditation status change takes place, Banks should be automatically and immediately notified, programmatically, in order for them to make the necessary changes to the API subscriptions of the TPPs in question. A push notification mechanism from the Directory to the Banks would be desirable, in order to enable the Banks to share data based on up to date accreditation information.

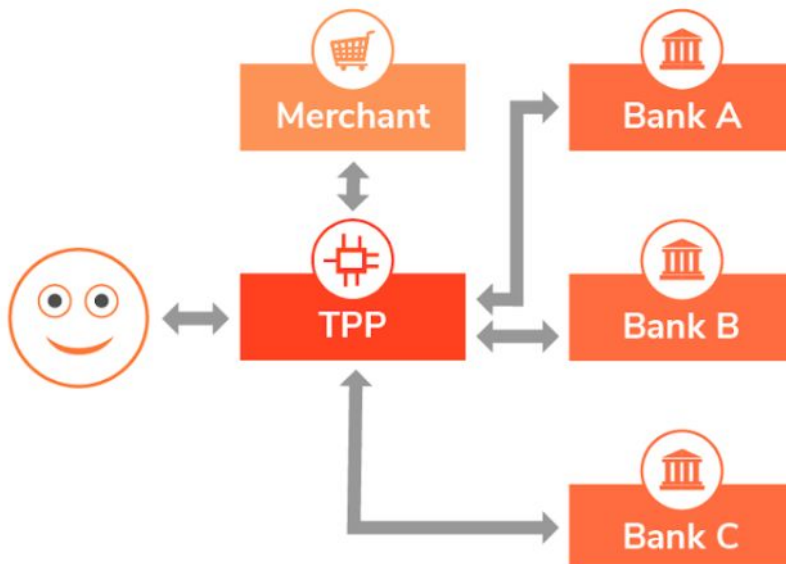
Incident Reporting

A mechanism for all the participants to report incidents to the regulator is also required. Banks will require the ability to report violations or abuse of their API platform by accredited TPPs. Conversely, TPPs will require the ability to report unavailability or connectivity issues of the Bank'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.

3.4. Recommendations on Security

Banks need to employ several mechanisms in order to ensure that the customer retains control of "who gets access to which data" in an Open Banking environment. This section details these varying requirements and considerations to be made in order to ensure a safe and efficient Open Banking ecosystem.

3.4.1. Authentication Mechanisms



Typically, an Open Banking transaction (be it an account information access or a payment initiation) is originated from a third party application since the customer consumes the banking products and services through a third party application.

Therefore, the bank needs to employ a direct channel with the customer in order to independently authenticate the user and obtain customer authorization for the desired data transfer.

In order to mitigate the risks of phishing and other attacks, Multi-factor Authentication (MFA) is recommended, which checks against a combination of something the user knows, something the user has or something the user is.

MFA, however, has the reputation of introducing a difficult user experience, especially since better customer experience is one of the main motivations of Open Banking. There are, however, ways of having a secure Open Banking ecosystem while maintaining great user experiences by employing variations of MFA techniques as well as adopting mechanisms such as adaptive authentication.

3.4.2. Consent Management

Once the customer is authenticated the bank then needs to proceed towards capturing explicit consent from the customer in order to either share data or initiate a payment. The consent capture should be fine-grained and easy to understand in order for the customer to consent to a certain subset of data, to be shared for a certain period of time with a certain Third Party. If the consent is for a payment, then the customer should be able to provide consent either for a one-time payment, recurrent payment or scheduled payment (if those payment methods are allowed under the Canadian Open Banking regime). Once the bank captures the consent it should be able to store it and retrieve it anytime, in order to produce it in case there is a dispute.

Additionally, customers should be allowed to change or revoke consents provided for future transactions at any time. The banks should allow access to a portal (preferably through an existing internet/mobile banking application or via a customer call center) where customers can manage the consents they have provided to the bank.

Consent management has to be carefully reviewed from the perspective of joint accounts based on the permissions of each individual account holder.

Business Customers

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

3.5. The Scope of Data and Phasing

It is important to identify the scope of data that should be made available by banks via APIs. Every country has their own risk appetite and the scoping of open data largely depends on this. In some countries such as Malaysia, Open Banking is originally limited to product information, which does not require customer authentication or consent since product data is not financial information pertaining to a particular customer. In other countries such as Australia, the opening up of datasets are phased, wherein product information, as well as a limited set of customer data, are available via Open Banking channels in the first phase, with the later phases introducing more datasets that are more complex (such as accounts of minors, joint accounts, and corporate accounts).

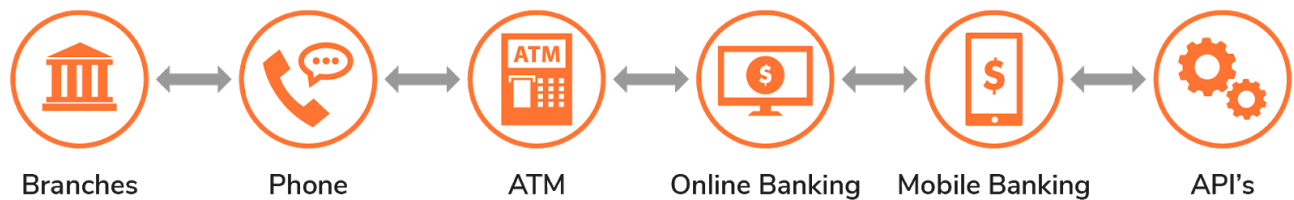
While phasing out the scope of data seems like a safe option to ensure that the Open Banking ecosystem starts small and progressively expands when it is mature enough to handle more complex datasets, there is a negative aspect to it from the banks perspective as well. Open Banking implementations take up a lot of time and effort especially to introduce new technology to open up APIs as well as to create the necessary integrations to the existing systems in order to make the data available as APIs. Many small to medium banks employ technology vendors to carry out these deployments and there is a cost involved each time a new dataset has to be exposed, especially if they are handled by different systems.

Therefore, WSO2 recommends careful consideration of the scope of data to be opened out as APIs. Clear guidance should be provided to banks well ahead of implementation deadlines so that they can make the right technology decisions from the beginning and plan out their implementation projects to minimize rework or continuous development.

4. Open Data - The Game Changer

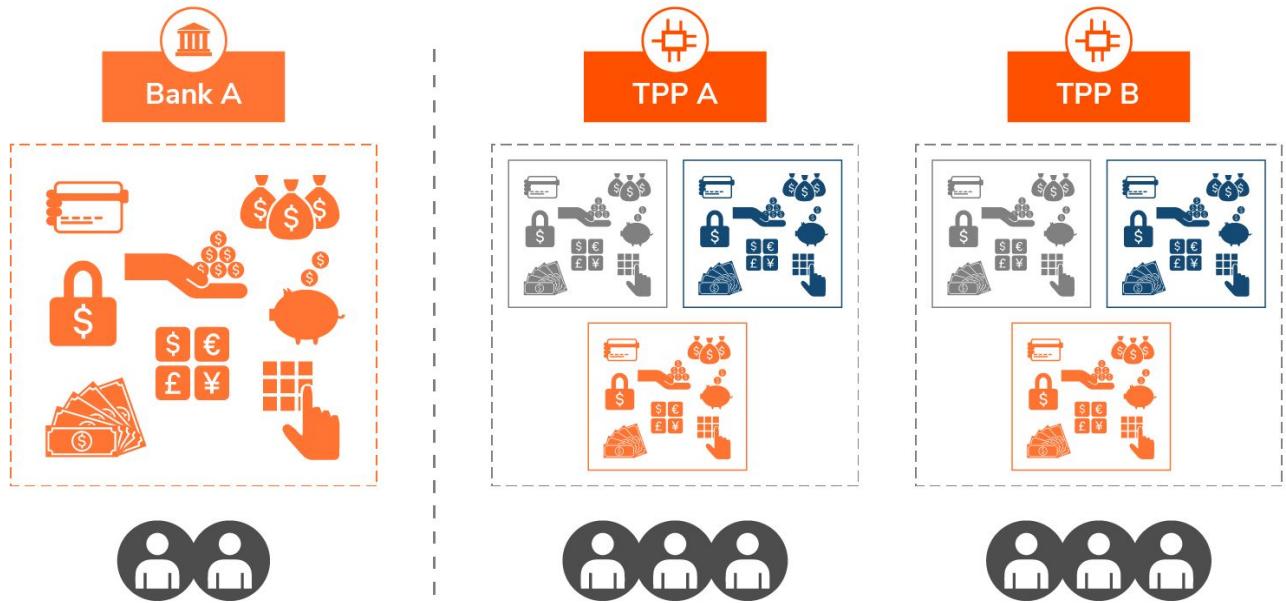
Open Data ecosystems undoubtedly unlock better experiences and better services for customers. It also opens up new business opportunities and access to new revenue streams to all the participants of the ecosystem. The following is a short commentary of the possibilities and the required technology capabilities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

4.1. Expanding the Distribution Channels



The above diagram shows the evolution of banking channels. All channels except APIs are provided by each bank, which means banks act as both the manufacturer and distributor of financial products and services. This means that the ability of a bank to provide financial products and services greatly depends on the bank's ability to create and maintain great distribution channels, which unfortunately is not a bank's core competency.

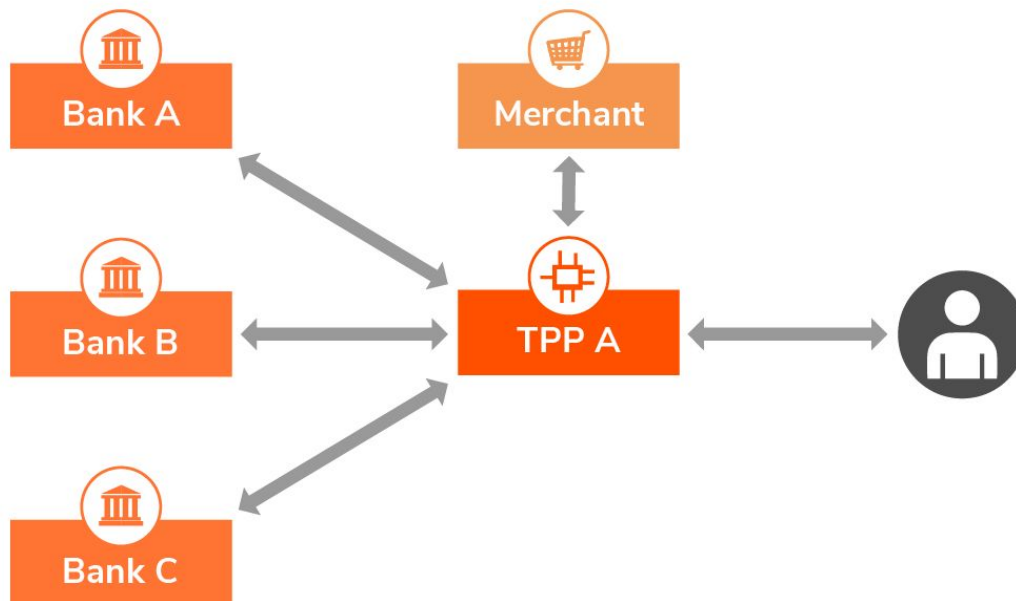
In the Open Banking world, the banking industry is able to operate like most other industries where there is a separation between the manufacturing layer and the distribution layer. This separation allows the manufacturers (banks) to focus on their key competency, making great financial products and services, while the distributors (TPPs) focus on theirs, making great customer experiences. This enables banks to now reach a much larger consumer group that was never before possible.



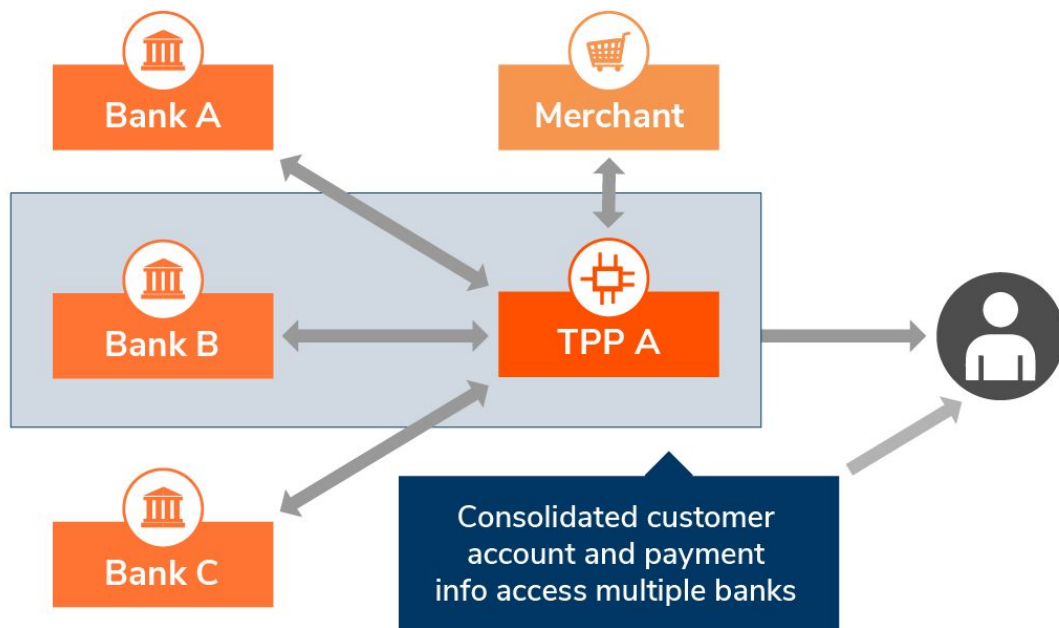
Maintaining a great API portal that enables TPPs to easily consume a bank's APIs is about the only requirement for banks to enable a large number of TPPs to take a bank's products and services to the masses.

4.2. Upselling to existing Customer Base

Most banks treat Open Banking as a compliance requirement with no real benefit to the bank.



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



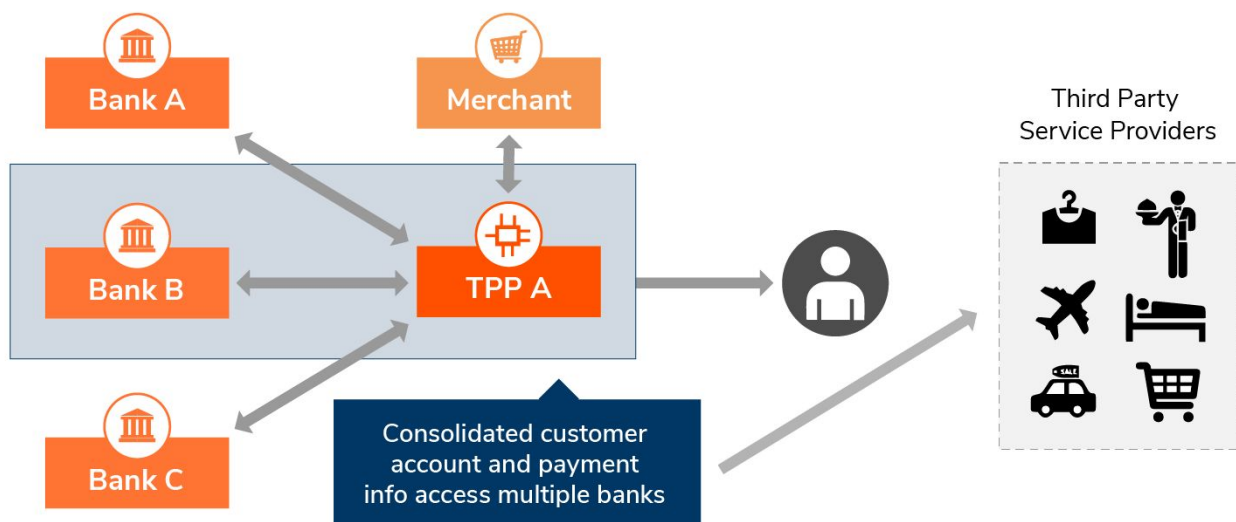
In jurisdictions such as Australia, the Open Banking strategy is created in a way that all banks that comply with Open Banking requirements are automatically accredited to function as TPPs. This increases competition between banks and results in better products and services for the end customer.

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 not just survive but thrive in this new ecosystem.

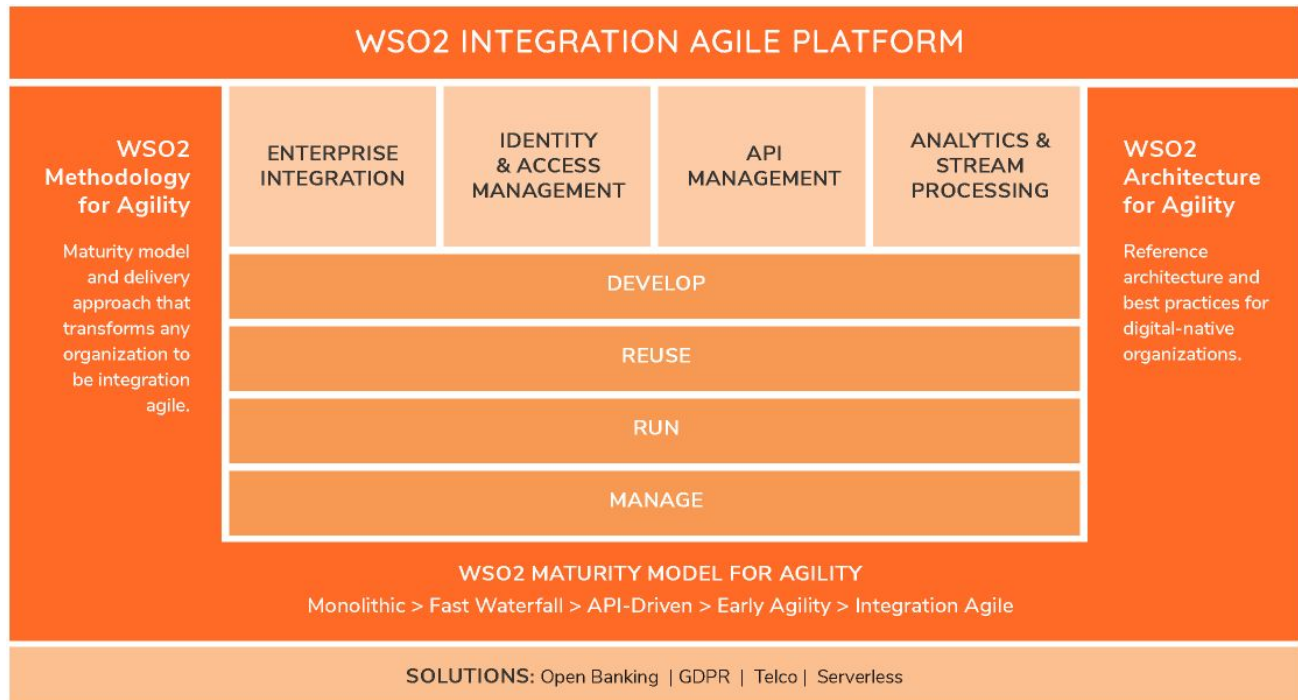
4.3. New Revenue Opportunities

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.



5. Technology for an Open Data Ecosystem



Open Banking taps into a vast amount of data that was previously held within the confines of a bank. If this data is analyzed carefully, a customer's preferences around everything such as travel, retail, and healthcare, can be understood and catered to.

While API's are the cornerstone of any Open Banking implementation, the bigger picture revolves around how you can take the data exposed by APIs and make sense of it in a way that allows you to create better experiences for your customers.

This involves:

- **Integration** - to connect to the thousands of APIs from multiple banks.
- **Identity and access management** - To ensure that the data flow and data integration within an Open Banking system adheres to customer consent.
- **Analytics** - To analyze and produce insights from data that helps you build products, services, and experiences that customers will be in awe of.

The key to capitalizing on the Open Data ecosystem is by investing in technology for the future. [WSO2 Open Banking](#) leverages the WSO2 Platform to provide a purpose-built solution for Open Banking. Since it is built on top of the WSO2 Platform, it can easily extend to meet any technology requirement beyond Open Banking. Our vision is to help enterprises in their journey towards becoming integration agile. Since the success of Open Banking extends beyond APIs towards an ecosystem centered on integration, this vision combined with our expertise in the domain make WSO2 the ideal partner for Open Banking implementations

6. Glossary

| Acronym | Definition |
|---------|------------------------------------|
| API | Application Programming Interface |
| CMA | Competition and Markets Authority |
| MFA | Multi-factor Authentication |
| PSD2 | Revised Payment Services Directive |
| TPP | Third Party Provider |