Review into Open Banking in Australia - -Recommendation Submission

SunTec Business Solutions

The power to xelerate

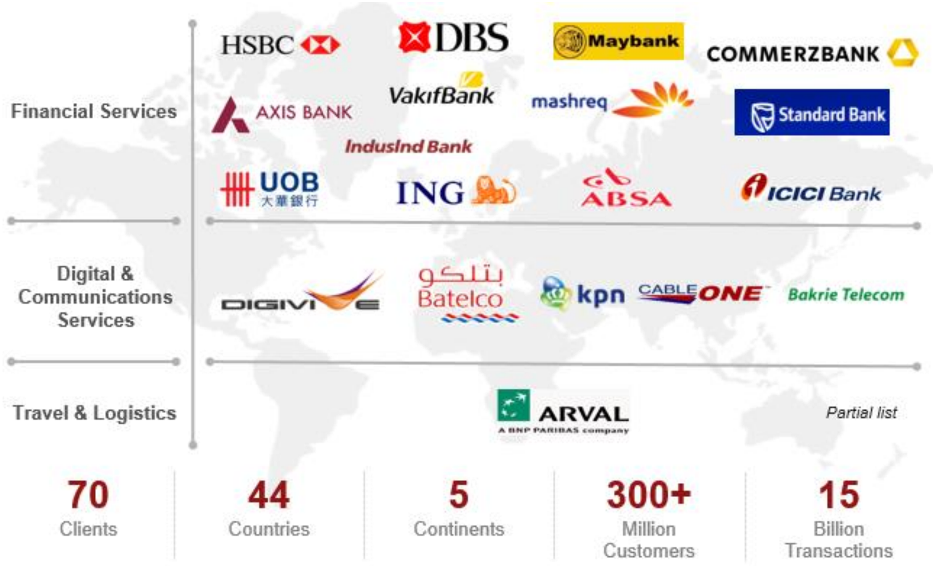
SunTec™

www.suntecgroup.com

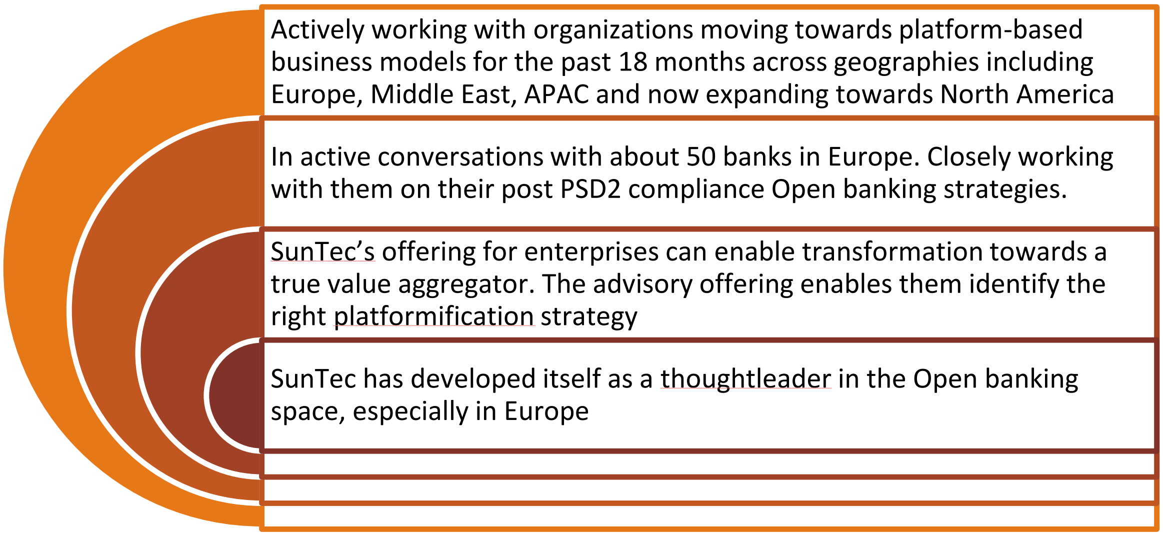
Contents

1 About SunTec Business Solutions

At SunTec Business Solutions, we help our clients increase the lifetime value of their customer relationships through effective revenue management and real-time customer experience orchestration. With a legacy of about 70 deployments in over 44 countries, SunTec is a trusted partner to some of the world's leading banks, digital and communication services, travel, and retail providers. Headquartered in India, we have our offices in the USA, UK, Germany, UAE and Singapore.



1.1 SunTec's play in the Open banking space



Actively working with organizations moving towards platform-based business models for the past 18 months across geographies including Europe, Middle East, APAC and now expanding towards North America

In active conversations with about 50 banks in Europe. Closely working with them on their post PSD2 compliance Open banking strategies.

SunTec's offering for enterprises can enable transformation towards a true value aggregator. The advisory offering enables them identify the right platformification strategy

SunTec has developed itself as a thoughtleader in the Open banking space, especially in Europe

2 SunTec's recommendation for Open Banking in Australia

At the onset SunTec would like to thank the Australian government for this opportunity to state our views on the CDR regulation and the following Open Banking Review in Australia. SunTec Business Solutions has been closely working on Open Banking for the past 18 months and has been in active conversations with key banks in Europe and other geographies to enable them achieve their open banking and platformification strategy.

Through this document the SunTec team has made a best possible effort to provide our views on the regulation. We would be pleased to be part of any further conversations that the Government might want to have, to understand our view better on the subject and the recommendations made in this document as follows. We have listed out specific sections in the report, where we had a recommendation to make as follows:

2.1 The potential of Open Banking

- Open Banking should allow the third-party participants/participants on the platform to collaborate with each other and co-create solutions that can cater to the larger consumption value chain of the customer, thereby enhancing the customer experience.
- Likewise, the bank providing the platform should be able to monetize the partnerships with third-parties, so as to incentivize banks to invest in creating these platforms
- The various revenue models between the banks and the third parties should be able to fuel competition between the third parties, so as to ensure that there is no cartel created at the background, and the consumer is truly benefited by willing to share his/her data with third parties
- The banks and the platform participants should be guided by a minimum level of transparency that they should abide by so that the customers have a view on the pricing as well as terms and conditions, and therefore has the real freedom of choice between various products, services and solutions

2.2 Open Banking regulatory framework

2.2.1 The legislation

- A tiered/layered approach of legislation for the CDR would be ideal considering the law is going to be applicable across sectors.
- The ACCC and OAIC should lay out the common regulations that will be applicable across sectors, thereby setting the objectives of customer experience, customer data privacy as well

increased competition and opportunities. This should then branch out to sector-specific regulations.

- The sector-specific regulations should be laid out in consultation with the regulatory bodies that are specific to the respective sectors like ASIC, APRA, RBA and others for Open banking specific regulations. This is to ensure that the nuances of the processes within the sectors are amply addressed.

2.2.2 Standards

- In addition to transfer, data and security norms, the standards should also include norm for data consumption which should cater to the techniques using which the data can be consumed. The purpose of this is to avoid data leakage and unethical consumption of the data

2.2.3 Compliance

- Compliance should be controlled by a central licensing regulatory authority which performs the due-diligence of the third party (external party who is going to consume the data).
- Compliance standards for licensing should be published to third-parties upfront.

2.3 The scope of Open banking

2.3.1 What types of data should be shared?

- Customer data when shared can be routed through the Central bank data source, so creating an opportunity to maintain the country's banking customer DB centrally.
- All amends to the records should be updated centrally.
- The data accessed for a particular request should not be further routed or used without the customer consent.

2.3.2 Who should be able to direct data be shared?

- Authenticated and Non authenticated access list to be maintained as a central repository by the governance or Central bank.
- Authenticated entities, for example, Tax authority can have access to the customer data without customer consent. While non-authenticated entities like competitor bank or fintech should be authorized by the customer for data access.
- The regulatory bodies should create logical categories to which the third-parties could be tagged. Each accredited third-party should be tagged under one or multiple categories based on the category criteria. Customer while approving data access should also be allowed to decide on

which category of third parties the data may/may not be shared with. This will provide the customer greater control of their data and the subsequent offers they are willing to receive from third party organizations.

- APIs for data sharing can be of three types within Open banking - Personal, Private and Public APIs. Each customer should have a personal APIs with an ID, this is a one-on-one link to customer ID.
- Whenever that APIs is called or consumed there is an alert or an event is logged.

2.3.3 Who can receive shared data?

- Authenticated entities, for example, Tax authority can have access to the customer data without customer consent. While non-authenticated entities like competitor bank or fintech should be authorized by the customer for data access.

2.3.4 Recovering the costs of data transfer

- Purpose of data transfer should be defined and can be a published and growing list. Basis purpose and parties involved the cost of such transfer can be apportioned and can be made transparent.
- Tariff model for Partner (Third party providers), APIs etc. should be maintained under Partner Contract, Business Service respectively for defining transparent monetization on usage of such service. For example, when you move your mortgage from one bank to another the cost of such transfer is borne largely by the customer and the new bank which is taking over, this is prevailing in most markets as of today. The data share for whatever be the purpose should be no different.

2.4 Safeguards to inspire confidence

- Tracking the true consumer of your customer data should be mandatory and made transparent to the customer. A fintech can possibly operate out of Sydney but can have operation unit in other parts of the world. The data when moved to other location for further processing or servicing should be consented for usage outside Australia. And systems should be able to track the data flow beyond the local office.

2.4.1 Addressing the risks in Open Banking

- Transactional data history should be linked to the product in context. E.g. If its Mortgage or recurring deposit that is being evaluated for better pricing elsewhere, then the data from the initiation date should be provided for better evaluation and pricing by the potential new bank.

2.4.2 Safeguarding the privacy of individual customers

- Clear definition of customer data, transaction data and aggregated data is important. Transaction data cannot have more information beyond the customer ID or account number. Definition is important primarily to avoid customer data going under transaction or aggregated data set.

2.4.3 Liability framework

- On-Us and Off-Us transaction classification for better tracking of liability. For e.g. if the transaction is initiated by the customer from the bank's side, the bank is liable to ensure the transaction is managed until its end state which can be outside with its partner entities. In the case of Off-us, the transaction can be initiated from a fintech portal by the customer and the request can flow into the bank from the fintech as an API, in which case the fintech is liable to ensure the transaction is managed until its end state which can be with other partners and possibly with a bank as well. Such arrangements have to be clearly captured as part of partner contracting to ensure the information flow, data liability and digital tracking of such flow of customer data is well managed in the open banking context, thereby protecting the customer.

2.5 The data transfer mechanism

2.5.1 Third parties need a dedicated interface

- Banks or data holders should be mandated by the regulatory bodies to share data only through dedicated APIs that abide by the security standards set. Screenscraping as a means of data sharing technique should not be acceptable as it would encourage the digital data thefts