GLOBAL BANKING & Finance review®
Global Insights & Analysis of the Financial & Business Markets

Is Regulatory oversight the biggest threat to undermining Open Banking

By **Brendan Jones**, Chief Commercial Officer of Konsentus

This article is in response to one from Matt Cockayne of Envestnet Yodlee published 5th October 2018 that stated the biggest threat to open banking was the lack of the FCA in the UK to extend the definition of an AISP to include non-consumer facing data aggregators.

And thus, by implication state that Yodlee and similar data aggregators that do not deal directly with Payment Service Users can not be regulated by them as AISPs.

I would push back on this premise in two areas, firstly to some of the arguments he states and then more importantly by highlighting what is a far bigger threat to open banking.

The Role of UK OBIE

Matt states that the Open Banking Implementation Entity (OBIE) only allows companies registered with the relevant regulatory authority (the FCA in the UK), to directly access Open Banking APIs in the long-term. Without this direct access, third party providers must register such companies as their 'outsource provider' so they can gain access to the Open Banking APIs indirectly."

I would contend that there is significant misunderstanding of the role of UK OBIE here. UK OBIE was created and mandated by the UK Competition and Markets Authority (CAM) for the 9 largest banks in the UK, commonly referred to as the CMA9, to be a member of and implement Open Banking standards under their instructions and directions. There is however NO mandate for any Third Party Provider (TPP) to register with UK OBIE to gain access to any Financial Institution (FI) the UK – FI's of course as term also cover Electronic Money, Payment Institution, Building Society and Credit Card accounts, under the European Payment Services Directive 2 (PSD2) open banking. For the UK market OBIE is purely a voluntary registration, despite what some banks or others would state.

The European Banking Authority RTS of Strong Customer Authentication and Common Secure Communications is very clear in that once a TPP has been approved/registered with their local National Competent Authority (NCA) and passported to the relevant NCA in the country of operation of the FI, then the FI cannot refuse access to the TPP unless they believe there to be fraudulent activity. If Envestnet Yodlee was registered with another countries NCA and then passported into the UK no UK FI can refuse it access.

Payment Service User Confidence

Matt states in the article that the current position of the FCA in not allowing aggregators to be AISPs will undermine confidence in open banking as "in the event of a data breach with an aggregator – consumers would not be able to hold that company liable." This is wrong, Payment Service Users (consumers, small and medium enterprises etc.) would never have a relationship with an aggregator service. Their contractual relationship will be with the TPP, for whom they have given their "explicit consent" to access their account(s) and who is providing the service. It is thus the TPP who as the direct contractual relationship that would be held liable by the Payment Service User (PSU) in the event of any data breach either at the TPP or any of their suppliers. It is a bit like a retailer and a wholesaler, the PSU has a relationship to the retailer, in the event that there is a problem they go back to the retailer not the wholesaler. It is up to the retailer then to take the dispute up to the wholesaler. Further the aggregator is likely to be also affected by GDPR legislation around the data breach and face regulatory oversight from this perspective also.

I can fully understand why Envestnet Yodlee would like to be regulated as it would make their business model easier to run in the UK, but to state it is the biggest threat undermining open banking implies that the majority of TPPs will use aggregators such as Envestnet Yodlee to access FI data and not just integrate directly with them – something that I believe a great many TPPs will do. Thus, the impact of any non regulation of aggregators will be limited both

by the number of TPPs using such services in the first place and the fact that they are covered by GDPR requirements already around protection of data.

The Real Big Threat to Open Banking

There are 9,000 plus FIs in Europe that need to be ready by March 14th 2019 for open market testing under mandatory PSD2 timescales. The biggest single threat to PSD2 open banking is simply the market will not be live and ready in time.

- To date there are still a number of countries that have not transposed PSD2 requirements into national law including Romania, Sain and Ideland.
- To date there are a number of NCAs who have not yet announced how they will register or approve TPPs, how they will hold the data and how they will communicate revocation.

Checking of TPPs identity and regulatory status is at the heart of PSD2 open banking.

When a PSU signs up to use a open banking service, they do not need to check that the service provider that they have provided "explicit consent" too, is regulated/approved, or indeed maybe a fraudulent, TPP; this is the job of the FI.

It is the job of the FI to check on the identity of the TPP and check their regulatory status, this is crucial to establishing the trust factor as part of the PSD2 open banking. As Matt stated "The data sharing aspect of Open Banking is already a primary concern for consumers – recent **research by Accenture** found that 85% of those asked said the fear of fraud would put them off sharing data, and 69% said they would not share financial data with businesses that were not banks." This means that all FIs need to ensure that they only ever supply PSU data to approved/regulated TPPs. If they supply data to a TPP who is not, then they are in breach of PSD2.

With Konsentus providing the only real time, online, machine readable database currently for the market covering both TPP regulatory status and eIDAS identity checking, we believe the biggest threat to PSD2 open banking is ensuring the NCA databases are ready and that FIs understand the importance of checking on TPPs.