

Meeting Summary of the Open Forum on Open Banking Information Session, 12 June 2018

Over the past few years, it has become a tradition for the Euro Banking Association to provide EBAday attendees with insights into its Open Fora stream via a breakfast session. This year in Munich, Open Banking Forum moderators Don Ginsel (Holland FinTech) and Gilbert Lichter (EBA) welcomed all early birds to a global tour de table on the topic of Open Banking.

A panel of experts from the US, India and Europe reported on initiatives and concrete deliverables in their home markets. While the specifics may vary from one country to the next, the key questions in Open Banking were the same across markets: What do customers want and how can we protect their interests?

Strategic approaches to Open Banking – a US perspective

Russ Waterhouse of US banking association and payments company The Clearing House (TCH) opened the discussion with a status report on data aggregation in the US market. Together with industry stakeholders, TCH has developed data aggregation best practices aligned with three core values: acting in the interest of customers, ensuring the stability and safety of the financial industry and fostering efficiency in the financial ecosystem.

Mr Waterhouse elaborated on data aggregation action plans the TCH has been pursuing to address privacy and security concerns. TCH approaches data protection from two angles. One is to develop core principles to guide the industry and ecosystem. This includes an integrated, bank-led viewpoint on key issues such as data aggregation principles, technical and security standards, and consumer education.

The second angle concentrates on creating a core industry infrastructure that can handle the increasing need for safety and security of customer data. Such an infrastructure should be able to respond to the customers' request for data transparency, access control and the ability to manage their permissions for data sharing with third parties. To that end, a certification vehicle – currently not available in the US – and assessments for trusted third parties as well as a central permissions hub need to be created. Mr Waterhouse introduced the audience to a customer permission portal model that TCH has conceived. Via an online bank account security dashboard, customers are able to see all third parties they have authorised their bank to share financial data with. From this dashboard, customers would also be able to add and remove third-party services.

Mr Waterhouse stressed that, in a hub-and-spoke model (with the bank as the hub that connects customers to the services of various specialised FinTechs), customers will ultimately hold the banks responsible for the protection of their data. Acting in the interest of the customers – both in terms of protecting their data and offering the services they desire – is thus essential to the success of any Open Banking model.

Digital India – an update

Parth Desai of payments solution provider Pelican started his presentation with an overview of government-supported digital payment offerings in India, including payment schemes, services and Apps. Over the last few years, India's digital payments landscape has been blooming, stimulated by various government-driven or -supported initiatives such as Aadhaar, a unique identification number for residents of India, DigiLocker, a government service that enables citizens to store official documents in a cloud, and the Unified Payments Interface (UPI), an instant payment system developed by the National Payments Corporation of India.

In addition to the improved digital infrastructure, the Indian payments industry benefitted from the explosion of smart phone use. Mr Desai used the example of 4G service JIO Mobile, whose low fees and smooth onboarding via e-KYC attracted 100 million new customers in only 170 days. JIO Mobile contributed to the proliferation of smart phones and boosted India to #1 in mobile data usage. Offering features such as e-wallets, special cash modes, and in-chat payment features, payments Apps such as paytm, Google TEZ, and WhatsApp are now highly popular among India's 400 million 4G smart phone users. This digital payment landscape is incentivised by both corporates (e.g. discounts for digital payments) and government (e.g. no service tax on digital transactions up to Rs 2,000).

While the digital payments and the digital economy in general have amassed an enormous amount of personal data, India currently lacks a larger data protection framework. Specifically, there is no law that protects the privacy and personal data of individuals. In 2017, the Indian Supreme Court ruled that Right to Privacy is to be protected by the Constitution. The government is now working on a data protection framework for India, which is planned to be delivered by the end of 2018.

Mr Desai concluded that despite growing fast and successfully, India's digital payments industry has a variety of challenges to face. In addition to the critical topic of data security, obstacles such as a persisting cash payment habit and limitations in reach due to lack of infrastructure in rural areas and illiteracy will occupy the industry for the next years.

PSD2 API interface – what does “good” look like?

In his capacity as co-Chair of the EU-API Evaluation Group, James Whittle of the UK's New Payment System Operator (NPSO), zoomed in on the challenge of compliance with PSD2, specifically the challenges of developing PSD2-compliant application programming interfaces (APIs). PSD2 requires banks to open the payment accounts of consenting customers to third-party providers but does not specify details of the APIs that third parties will use to connect to banks. Furthermore, APIs are not standardised across the EU. EU-wide initiatives such as the Berlin Group and national initiatives in Poland, Slovenia and France have been working on standardisation frameworks.

Mr Whittle reported on the status of the API Evaluation Group (API EG), a market-facing group that was proposed by the European Commission in November 2017 and has commenced its work in January 2018. The group's objectives are to define objective API

evaluation criteria, evaluate standardised API specifications, make recommendations towards API specification and provide a broadly supported source of market guidance.

At this point, the group conducted a first review together with API standardisation initiatives and collected information on what functionalities the various standardisation initiatives support. Furthermore, the group has been working on drafting guidance on functionalities and recently finalised and published guidance on authentication.

Payment initiation services in Europe – a status report from the ERPB Working group on PIS

Etienne Goosse, Director General of the European Payments Council (EPC), reported in the capacity of the EPC as acting secretariat for the ERPB PIS working group, on the current status of this working group.

After having issued a report to the ERPB for their November 2017 meeting, the ERPB mandated the working group to continue their work and review the recommendations on the envisaged requirements against legal certainty of the final RTS. Also, the ERPB supported that the working group continues the work on those requirements that need a follow-up, such as (1) the standardisation of PSD2 certificates (in liaison with ETSI), (2) the harmonisation of registers and the establishment of directory services and (3) the development of remaining business requirements. The working group was requested to provide an additional report to the June 2018 ERPB meeting.

The updated report now provides further clarification and requirements in relation to the identification of payment service providers (PSPs) relying on standardised certificates containing PSD2 data elements provided or made available by national competent authorities (NCAs) to qualified trust service providers (QTSPs), as well as in relation to operational pan-European directory services. It also further clarifies requirements for an efficient and well-functioning communication and resolution process for event and dispute handling between account servicing payment service providers (ASPSPs) and third-party payment service providers (TPPs).

The report was presented at the next meeting of the ERPB on 19 June 2018.

Thoughts to take to the next meeting

The moderators concluded the meeting by providing an outlook on future topics on the agenda of the Open Forum on Open Banking:

While customers want convenient and efficient banking services, data breaches affecting consumers and businesses alike have become more frequent and made people keenly aware of the value of their data. While convenience may still trump privacy in other industries, consumers expect that banks protect their personal data.

The consumer sentiment towards stronger data protection and control is notably growing across markets and will certainly affect the development of Open Banking. Regulation such as GDPR and PSD2 helps set the legal framework for the interaction of parties that data sharing processes require. However, as the reports on the work of the ERPB's PIS sub-group and the API Evaluation Group indicated, the practical success of Open Banking will



very much depend on the way these requirements are implemented – both at the level of the collective elements, such as standards and authentication procedures, and at the level of the resulting individual solutions. How to develop, implement and regulate Open Banking solutions that meet the requirements of all parties in terms of a wide range of topics, from cyber security to liability concerns, from convenience to data privacy, will give the Open Forum on Open Banking a plethora of topics to discuss in the future.