**Dr Andreas Fillmann** Partner
andreas.fillmann@squirepb.com
Squire Patton Boggs, Frankfurt

# Change brings opportunity: The EU banking ecosystem and the importance of APIs

New technologies, increased competition and a favourable regulatory environment are among the factors driving innovation across the financial services industry. Major banks and financial institutions are facing increasing competition from FinTechs that offer flexible products through digital banking apps, as well as from tech firms that are also entering the sector. Dr Andreas Fillmann, Partner in the Financial Services Practice and Member of the global FinTech Group at Squire Patton Boggs, provides insight into the opportunities presented by the revised Payment Services Directive ('PSD2') and Open Banking for banks and the importance of Application Programming Interfaces ('APIs') within this changing landscape.

Many FinTechs have been successful in providing customers with positive new banking experiences and so many large banking organisations view FinTechs not necessarily as competitors, but as potential partners, bringing smooth processes, an innovative culture and much needed technological expertise to the banks. The advantage that traditional banks still have compared to FinTechs is a better knowledge of financial regulations, greater access to capital, and the size of customer base needed to scale.

Further, blockchain - the shared, distributed ledger technology - is on the horizon for the financial industry and represents a vehicle for change. The ledger file is not stored in the servers of a central entity, like a bank, nor in a single data centre. It is distributed across the world via a network of private computers that are both storing data and executing computations. Each of these computers represents a 'node' of the blockchain network and has a copy of the ledger file. This distributed ledger technology has the potential to lead to significantly more decentralised asset ownership, but it is not expected to be ready and fully integrated with the banking environment anytime soon. It could take some time for blockchain technology to make a meaningful impact across the financial industry, whereas the Open Banking infrastructure is already at work.

Notably, Open Banking infrastructure will foster competition between banks and non-banks. There are potential benefits of an Open Banking infrastructure system that include improved customer experience, new revenue streams and a sustainable service model for underserved markets. In particular, open APIs will be used by FinTechs, but they can also help banks to maintain competitiveness, being an opportunity to acquire new business or reach out to new markets, offer customer-friendly services and speed up the development of internal systems. Simply ignoring Open Banking is not an option any longer for banks.

The industry is already aware that traditional business models are under threat from FinTechs becoming massively successful by offering something that solves customer needs. However, to succeed with the Open Banking infrastructure, banks themselves need to change their business models. They also need to think about their API strategy - will they be a simple transaction processor and leave the innovation to others? Alternatively, they could develop APIs in-house to add value for their business and customers or enter into partnerships with FinTechs to improve their customer base.

First, it is important to understand what an API in the banking environment means. According to the Euro Banking Association ('EBA')[1], an API can be seen as the interface between software applications, both within and between organisations. An API is "a way for two computer applications to talk to each other over a network using a common language that they both understand." Banks and other financial firms can use APIs internally, to integrate diverse systems and allow for the exchange of data across different departments, or externally, to expose business assets to external audiences. APIs create both risks and opportunities for players in the banking market. The risks are mainly related to privacy and data protection, especially in the EU considering the imminent application of the General Data Protection Regulation ('GDPR'), which imposes substantial penalties for non-compliance. These risks may not only relate to sanctions, but there are also risks relating to the potential loss of brand recognition and such reputational risks might impact customer loyalty.

Second, APIs enable secure, controlled and cost-effective access to data and/or functionality of systems. Furthermore, the term 'open API' refers to APIs that allow third party access to systems belonging to another organisation. However, an open API within the banking industry does not necessarily mean that any third party can freely access a bank's system without restriction. Banks should impose controls in order to preserve security, privacy and contractual assurance.

Third, it is important to categorise the types of open API in order to assess the implications, opportunities, risks and the priority for selecting and implementing them. Open APIs may be categorised as follows:

- Product and service information - 'read-only' information offered by banks providing details of their products and services;
- New applications for product and/or services - customer acquisition processes, such as allowing online

Image: NilsEisfeld / Moment / Getty Images

**Many large banking organisations view FinTechs not necessarily as competitors, but as potential partners, bringing smooth processes, an innovative culture and much needed technological expertise to the banks.**

submission/application for credit cards, loans or certain insurance products;
- Account information - retrieval and alteration (where applicable) of account information (balance, transaction history, limits, payment schedules, etc) of authenticated customers for standalone or aggregated views; and
- Transactions - payment or scheduled payments/transfers by authenticated customers.

Fourth, there are inherent risks associated with sharing customer data through APIs, which is why it is critical for the banking industry to develop processes and governance to secure such technical connections. Although the core API value proposition lies in streamlining the systems' integration required for data access, the need for rules and regulations to support the protection of the privacy and security of personal data create an infrastructure challenge for the industry.

Consequently, the Official Journal of the European Union on 13 March 2018 published the Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 for secure open standards for communication supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication. The Regulation is directly applicable in all EU Member States and sets out the requirements that payment service providers (e.g. CRR credit institutions) must meet in order to implement security measures that enable them to:

- Apply a strong customer authentication process;
- Refrain from performing the required strong customer authentication, subject to specified conditions;
- Protect the confidentiality and integrity of the payment users' personalised security features; and
- Establish common and secure open standards for communication under Title IV of Directive (EU) 2015/2366 ('PSD2').

This stricter approach to security will contribute to reducing the risk of fraud for both new and more traditional means of payment, especially online payments, and will protect the confidentiality of the user's financial data (including personal data). Payment service providers will be obliged to apply strong customer authentication when a payer initiates an electronic payment transaction. Strong customer authentication is an authentication process that validates the identity of the user of a payment service or of the payment transaction (more specifically, whether the use of a payment instrument is authorised).

Strong customer authentication is based on the use of two or more elements categorised as 'knowledge' (something only the user knows, e.g. a password or a PIN), 'possession' (something only the user possesses, e.g. the card or an authentication code generating device) and 'inherence' (something intrinsic to the user, e.g. the use of a fingerprint or voice recognition) to validate the user or the transaction. These elements are independent (the breach of one element does not compromise the reliability of the others) and designed in such a way as to protect the confidentiality of the authentication data. For remote transactions, such as online payments, the security requirements go even further, requiring a dynamic link to the amount of the transaction and the account of the payee, to further protect the user by minimising the risks in case of mistakes or fraudulent attacks.

Apparently, PSD2[2] aims to provide the legal foundation for the further development of a better integrated internal market for electronic payments within the EU. EU Member States had to enact national legislation by 13 January 2018 to implement PSD2. Even though API technology is not directly mentioned in PSD2, the Directive has adopted a programmatic approach by taking such technology into account. PSD2 aims to remove barriers to trade and foster innovation by forcing banks to open up their systems to non-banking companies.

According to Recital No. 33, 'the directive should aim to ensure continuity in the market, enabling existing and new service providers [...] to offer their services with a clear and harmonized regulatory framework. [In this context, each state] should guarantee fair competition in that market avoiding unjustifiable discrimination

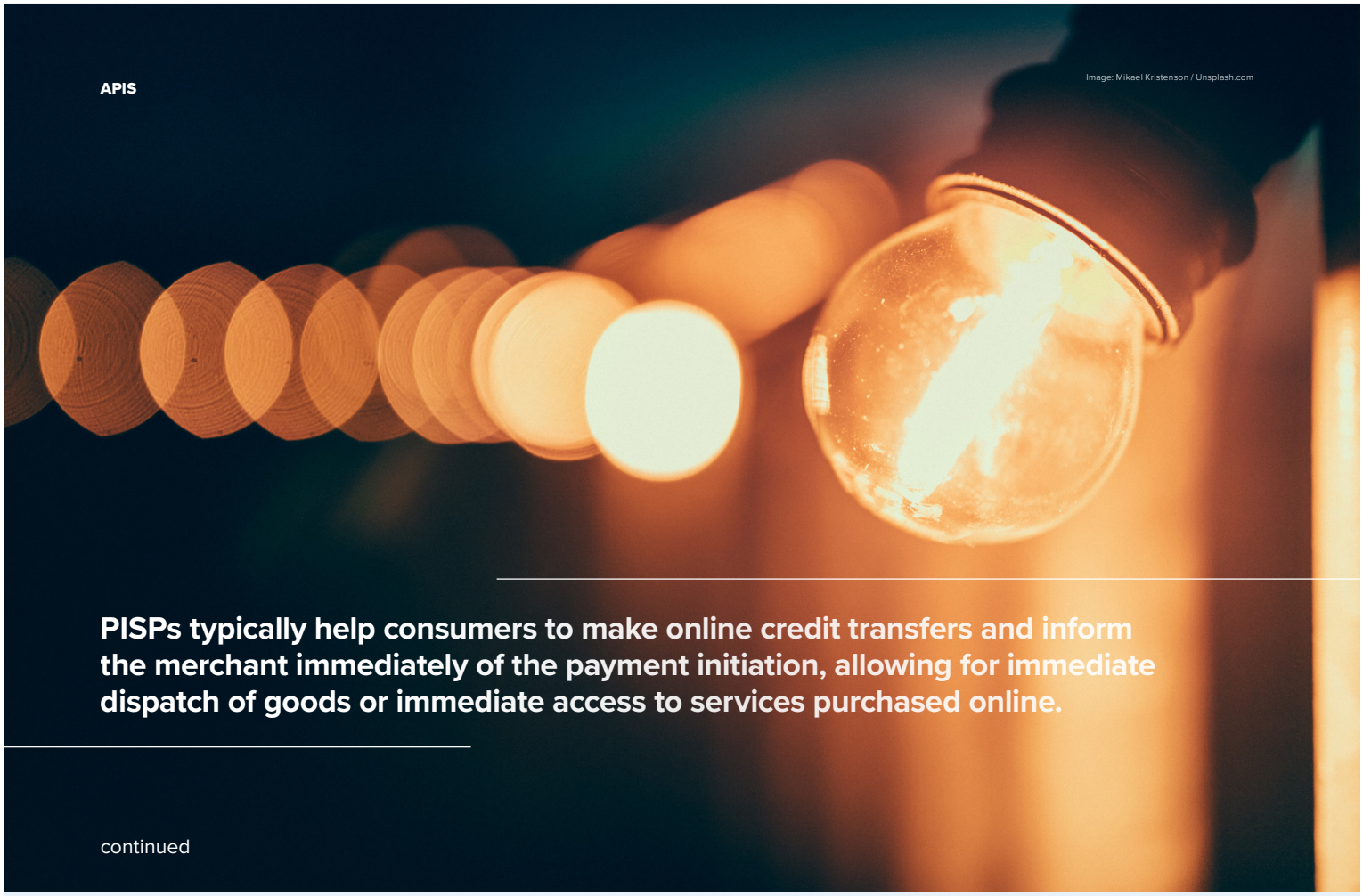

Image: Mikael Kristenson / Unsplash.com

**PISPs typically help consumers to make online credit transfers and inform the merchant immediately of the payment initiation, allowing for immediate dispatch of goods or immediate access to services purchased online.**

continued

against any existing player on the market. Any payment service provider, including the account servicing payment service provider of the payment service user, should be able to offer payment initiation services.'

Payment initiation service providers ('PISPs') and account information service providers ('AISPs') are online services that respectively provide the initiation of a payment at the request of the customer or aggregated information on one or more payment accounts held by the customer (e.g. balances, transaction history, etc). These services can only work if they are granted secure access to customers' accounts and payment services, provided by banks. The best way to ensure the latter is through open APIs.

The effects of PSD2 on competition are massive and even if the implementation and creation of an API framework could be burdensome for banks in the shorter term, the implementation costs would be largely outweighed by the benefits, in terms of the opportunities and innovations possible.

PISPs typically help consumers to make online credit transfers and inform the merchant immediately of the payment initiation, allowing for immediate dispatch of goods or immediate access to services purchased online. For online payments, they constitute a true alternative to credit card payments, as they offer an easily accessible payment service, as the consumer only needs to possess an online payment account. AISPs allow consumers and businesses to have a global view of their financial situation, for instance, by enabling consumers to consolidate the different payment accounts they have with one or more banks and to categorise their spending according to different typologies helping them with budgeting and financial planning. PSD2 requires that all payment services providers be authorised and regulated.

The inclusion of new payment providers within the scope of PSD2 will allow competent authorities to better monitor and supervise the activities of these new players. PSD2 also fully clarifies the liability issues between banks servicing the account of the payer and the payment initiation service. When a payer uses a PISP to initiate a payment, it is liable for any payment incidents within its sphere. In particular, the bank of the payer shall not be held liable for payment incidents that can be traced back to the initiator.

However, with PSD2, innovation has never been so accessible to banks and, aside from simply becoming compliant with the regulations, banks should actively build on this foundation to deliver more value add services and a better experience for their customers.

Banks now have the opportunity to utilise new distribution channels and take on different roles in the value chain. They have traditionally played the role of account service provider while FinTechs have been positioned as PISPs or AISPs. Maintaining the *status quo* has implications, though. Not taking advantage of the new roles and distribution channels will simply leave banks with the huge cost of compliance.

Yet, by becoming an AISP or PISP, banks can strengthen their customer relationships and enrich customer satisfaction. Furthermore, by creating APIs that source data from other banks (be it simple account information aggregation or new products developed elsewhere), banks will grow their distribution network via the third party ecosystem, will become more scalable and will create new value add capabilities, while still remaining secure.

1. 'Understanding the business relevance of Open APIs and Open Banking for banks,' Euro Banking Association, May 2016.
2. https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en