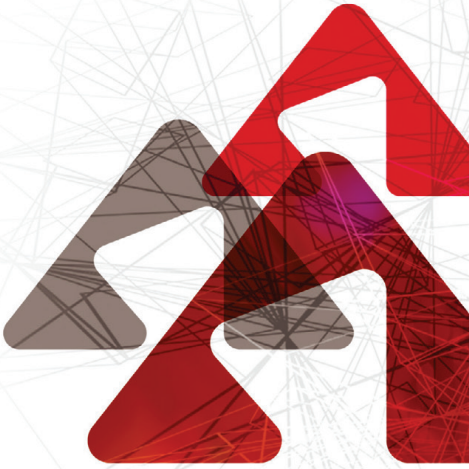
Galitt
Payment Consulting

PSD2 & OPEN API: threats and opportunities for the banking sector

Are we moving towards Open-Banking?



WHITE PAPER
December 2016

DE GAULLE
FLEURANCE
& ASSOCIÉS
SOCIÉTÉ D'AVOCATS

Contents

About this white paper & acknowledgements

Galitt, a company specialised in payments, and the law firm De Gaulle Fleurance & Associés have come together to bring you this white paper concerning Open-Banking and all the issues arising from France's implementation of the revised Payment Services Directive *(Directive 2015/2366)*, known as PSD2, which will revoke the original Directive 2007/64/CE *(PSD1)*, currently in force in France as it becomes part of monetary and financial law.

We would particularly like to thank the following people for their participation and expertise:

Joan Burkovic: *CEO of Bankin'*

Joan Burkovic, who graduated from ESSEC and HEC Lausanne, co-founded Bankin' with Robin Dauzon in 2011. He is also one of the founders and board members of the France Fintech association, as well as being a spokesperson for European AIS, which brings together those involved in bank account information services across Europe.

Bankin' is an app that works as an intelligent, personal finance coach, in order to help its users to manage their daily finances better. It is currently available in four countries: the UK, Germany, Spain and France and count over 1.5 million users.

Sébastien Taveau: *Chief Technologist at Early Warning*

Sébastien Taveau is the Chief Technologist at Early Warning, where he supervises technological and innovative operations for P2P payment solutions. With over twenty years of experience in the field of mobile payment technology, he sees himself as a puzzle-solver and a look-out, scanning the horizon. Sébastien Taveau is an acknowledged expert in Open API, with numerous articles and appearances on CNN, The Wall Street Journal, The Huffington Post, Mashables, Reuters, Forbes, Dark Reading, Digital Transactions, Newsweek and more.

Early Warning is specialised in mobile payment technology. Founded 25 years ago by Wachovia, JPMorgan Chase, Bank of America, BB&T Corporation and Wells Fargo, Early Warning is still at the centre of events with the launch of Zelle.

Jérôme Raguénès: *Director of Digital Coordination at the French Banking Federation (Fédération Bancaire Française - FBF)*

Jérôme Raguénès is the Director of Digital Coordination with the managerial board of the French Banking Federation since November 2015. He is a member of the Digital Strategy group on the executive board of the European Banking Federation.

He has almost twenty years of experience in the field of payment means and systems. As a consultant for ten years on important strategic projects for large banking groups, he was asked by the FBF in 2002 to coordinate the SEPA project, to take charge of the regulatory files for payment means and to look after the interests of the French banks with both national and European institutions.

The French Banking Federation *(FBF)* is a professional body representing every bank present in France. It currently acts for 378 banking institutions of all types *(commercial, cooperative and mutual)*, both French and from overseas.

FEDERATION
BANCAIRE
FRANCAISE

About De Gaulle Fleurance & Associés

The low firm De Gaulle Fleurance & Associés *(Paris and Brussels)* now counts over 110 lawyers and legal professionals, of whom 40 are partners.

All our lawyers boast cross-disciplinary skills, allied to one or more fields of excellence *(for example, public and administrative law, intellectual property, banking law, new technologies, tax, commercial law, corporate structure, etc.)* in terms of both advice and disputes, including on an international level.

The low firm De Gaulle Fleurance & Associés is organised around two specialist services:

- the structural service is designed to meet clients' needs concerning human and social capital and the governance thereof, whether those clients be public or private sector. It takes care of all of the organisational side, including optimising structures and the best use of a company's skills capital;
- the operations service is dedicated to public or private sector clients' operational needs, including managing human resources, mobilising finance and optimising decision-making processes.
  To find out more: www.degaullefleurance.com

Contact:
Thibault Verbiest
Partner
+33 6 25 44 12 71
tverbiest@dgfla.com

About Galitt

The reference in the field of electronic money and transactions, Galitt is the market leader in France in every one of its business sectors, and throughout the world for its testing tools and its expertise in innovative technology.

Galitt is recognised for offering a wide range of skills and complementary knowledge to assist its clients throughout the lifecycle of their projects and in every link of the payment value chain. The company's size allows it to take on large projects while retaining its ability to be reactive, its personal touch and the ambition of an organisation that is run on a human scale.

Galitt is the benchmark in the execution of the most advanced payment technologies and the definition of tomorrow's technological architecture.

Galitt's services are based around 5 Business Units:

- **Payment Consulting** experts and their innovative approaches inform and enlighten our clients' strategic decision-making;
- **Payment Services** consultants help our clients with the execution of their payment projects;
- **Testing Solutions** consultants help our clients with the execution of their payment projects;
- **Payment Solutions** teams develop testing software and take part in both the industrialisation phase of testing and the certification of solutions;
- **Payment Education** trainers pass on Galitt's expertise and experience during our training seminars.

In 2015, Galitt achieved a turnover of €31 million and employed 240 people. To find out more about Galitt, please visit our website, at: www.galitt.com

Contact Galitt Payment Consulting:
Rémi Gitzinger
Directeur Exécutif
+33 6 20 66 77 40
r.gitzinger@galitt.com

Background

Proposed by the European Commission, passed by the European Parliament in 2015, and due to become part of French law by January 2018 at the latest, the PSD2 Directive paves the way, in regulatory terms, for a new notion: Open-Banking. From now on, customers will gain the right to have their banking data at their disposal, which could force banks to make the data available to third parties, via Application Programming Interfaces *(APIs)*, with the primary goal of stimulating competition and innovation in the banking sector.

This situation of opening up banking data and making it available to third parties has raised several questions and controversies in France and across Europe, which we will study closely in this white paper.

Issues

With PSD2, how can rights of access be transposed into national law, and what impact will they have on the banking ecosystem?

Firstly, we will analyse the legal implications. In order to bring a wider viewpoint to the white paper, we have carried out three interviews, which lay out what is at stake for different stakeholders. Secondly, we will study the new ecosystem which is being developed in Europe, and we will look more closely at both the technical and operational consequences. Finally, in the third part of the white paper, we will set out the stakes for the banking sector as a whole, and look at the different initiatives which are already springing up.

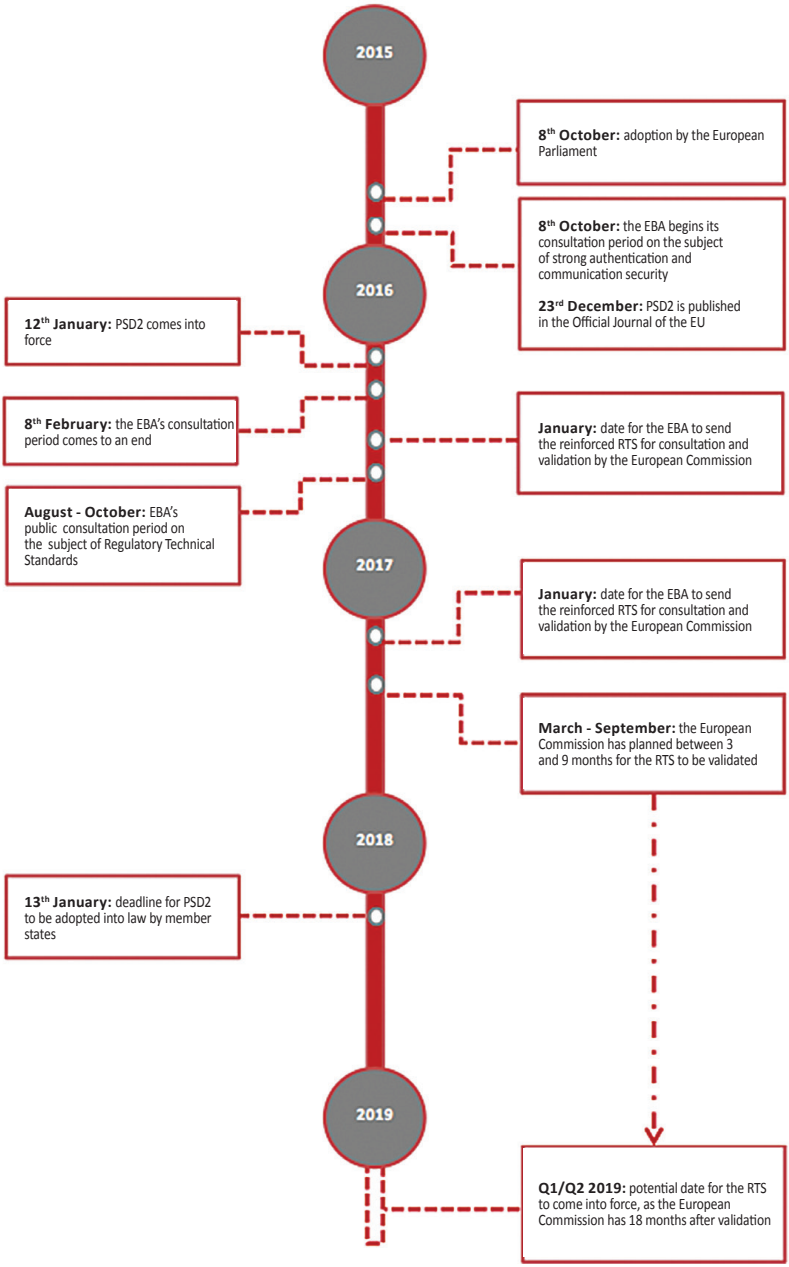
So as to keep the various deadlines of PSD2 in mind, a calendar of the Directive's implementation is available in this white paper. October 2016 represented an important step forward in the calendar of PSD2. It marked the end of the consultation period of the European Banking Authority *(EBA)* with banking firms. Launched in August 2016, this consultation period was aimed at collecting the opinions of all stakeholders concerning regulatory and technical aspects, linked to the requirements for strong authentication of customers and the need for greater communication security contained in the directive.

Definitions from the European Banking Authority [1]

- **EBA** *(European Banking Authority)*: a body which is independent of the European Union, and which works to guarantee standards of regulation and efficient, coherent prudential supervision across the entire European banking sector..
- **RTS** *(Regulatory Technical Standards)*: the overall body of technical standards prepared by the European Banking Authority, in collaboration with the ECB *(European Central Bank)* and the National Central Banks. These technical standards are agreed with a wider audience of stakeholders via "discussion papers". They are mainly concerned with strong authentication and secure means of communication, so as to enable the operational implementation of the Directive. These standards will be submitted to the European Commission in 2017 for regulatory enforcement.
- **API** *(Application Programming Interface)*: the general, normalised group of classes, methods and functions used in order to have access to services and to data. These interfaces have to be scalable, reusable and secure, all whilst offering ease of use to IT developers.
- **Open API:** a principle which consists of making a programming interface available to authorised, extern, third parties, thus giving them access to internal data and/or services, in order for them to meet any needs arising.
- **Open-Data:** a concept which deals with opening data up, so that it is freely available, usable and reproducible by all, with no restriction on ownership, copyright or any other control mechanisms.
- **Open-Banking:** a concept which is currently still being developed, concerning the future of banking. Open-Banking is based on the principle of banking transparency; it advocates using Open APIs in order to give third parties access to information which can help them with the development of their own applications.

*1 - **EBA** : Definitions / Open APIs and Open-Banking*

TIMELINE OF KEY DATES FOR PSD2



1. The legal framework

1.1. Some definitions set out by PSD2

- **PSU** *(Payment Service User)*: a private or professional user possessing one or more bank accounts and/or the user of a payment service.
- **ASPSP** *(Account Servicing Payment Service Provider)*: a provider of a service within which a customer *(PSU)* holds one or more accounts and/or within which the PSU initiates payments. Each ASPSP must hold the status of Payment Institution *(PI)**, with potentially the passport that would allow them to operate in different countries; credit institutions, electronic money institutions and payment institutions which already hold this status are considered as being ASPSPs.

> * ***Clarification – Payment Institution (PI):*** *these were created following the first Payment Services Directive (PSD) in 2009. Previously, only banks and credit institutions were authorised to provide payment services. With the growth of online payment, new, smaller firms have been able to gain this status so as to bring greater competition to the sector. The status is accorded by the financial authorities of the country in which the request is made; in France, this means the ACPR (Autorité de Contrôle Prudentiel et de Résolution), connected to the French Central Bank. Gaining and keeping the licence is subject to rigorous procedures in order to provide Payment Service Users with strong guarantees.*[2]

- **TPP** *(Third Party Provider)*: a service provider who is able to initiate payments at the request of the payer, without holding the funds and from accounts which the provider does not manage. A TPP can also provide consolidated information concerning these accounts.

This comprises the following two categories of service provider:

- **PISP** *(Payment Initiation Service Provider)*: a provider which offers a service that can initiate a payment order, at the PSU's request, from a bank account which is held by an ASPSP.
- **AISP** *(Account Information Service Provider)*: a provider which brings an information consolidation service concerning one or more accounts held by a PSU with one or more ASPSPs.

2 - ***ACPR*** *: Clarification of Payment Institution*

Without doubt, the main innovation that PSD2 brings, and the one which has caused the most heated debate, is the recognition of these two new payment services, allowing a third party to position itself between a user and his/her ASPSP: the payment initiation service and the account information service.

The new Payment Service Providers can take advantage of lightened operating conditions and softened prudential requirements, when compared to ASPSPs. They will, however, just as for other Payment Institutions, be subject to licensing controls *(they will be registered for the Account Information Service)* and will need equivalent professional and public liability insurance covering all the jurisdictions in which they provide services. The minimum amount for this will need to be defined according to criteria established by the EBA's forthcoming guidance.

1.2. Rights of Access

Articles 66 and 67 of PSD2 set up, firstly a right of access to payment accounts for Payment Initiation Service Providers *(PISPs)*, and secondly, a right of access to the payment account information for Account Information Service Providers *(AISPs)*.

These access rights come with a certain number of guarantees:

1. Access is limited to only payment accounts which are accessible online;
2. The explicit consent of the Payment Service User *(PSU)* is required for each transfer of his/her account's information;
3. PISPs may not hold the payer's funds;
4. Personalised security data *(credentials)* are not accessible by third parties, and their transmission to both the user and the issuer must be via effective and secure channels;
5. Communication must be secure between the Account Servicing Payment Service Provider *(ASPSP)*, the payer and the payee only, and must conform to the EBA's future Regulatory Technical Standards *(RTS)*;
6. No modifications may be made by PISPs to the characteristics of the operation *(total amount, payee, etc.)*;
7. AISPs may only have access to information originating from the designated payment account, and its associated payment operations;
8. PISPs may not store sensitive payment information concerning the PSU; the expression "sensitive payment information" means "data, including personalised security data which could potentially be used to commit fraud". This category covers personalised security data, though it excludes - but only where AISPs and PISPs are involved - the account holder's name and the account number;

9. AISPs may not request transmission of sensitive payment data connected to payment accounts;
10. Only information which is essential to the provision of either payment initiation services or account information services may be requested from the PSU;
11. Use, consultation or storage of data may only be done with the intention of providing either Payment Initiation Services or Account Information Services;
12. ASPSPs must have the ability to refuse to give PISPs and AISPs access to a payment account, for objective and documented reasons, linked to an unauthorised or fraudulent attempt at access, including an unauthorised or fraudulent initiation of a payment operation.

1.3. Is using payment data for commercial ends to be banned?

PSD2 doesn't expressly outlaw the use of payment data for commercial ends *(unlike the Anti-Money Laundering Directive)*. The real issue is the ownership of banking data and its re-use by new companies in the realm of Big Data. However, articles 66 and 67 of PSD2 should be interpreted as prohibiting the use of banking data for commercial ends:

- the PISP "may not use, consult and store data for purposes other than the provision of the Payment Initiation Service expressly requested by the payer" *(art. 66, § 1, g)*;
- the AISP "may not use, consult or store data for purposes other than the provision of the Account Information Service expressly requested by the Payment Service User, and conforming to the rules relating to data protection" *(art. 67, §2, f)*.

Apart from this legal clarification, it's important to stress that third party service providers were growing quickly in number well before the Directive came along. The European Commission wished to intervene in order to regulate these new practices, and had the major objectives of creating a new, more adapted, regulatory framework and of promoting their development in a spirit of free competition.

These new firms, their service offers and their integration into the payment chain are described and analysed in the second part of this paper. There will also be an explanation on the subject of technical repercussions of the sharing of banking data.

INSERT 1 INTERVIEW

Jérôme Raguénès

Digital Coordination Director - French Banking Federation

Galitt: *Could you explain to us how the banks feel about the influx of all these new companies, whose arrival has been facilitated by the growth of the digital sector and the new regulations?*

Jérôme Raguénès: The banking sector is very competitive, and is becoming even more so via the successive introductions of restrictive regulations that have allowed new firms to come and compete with banks in several of their core sectors:

- in financing services: the tightening of banking regulations has led to the growth of new ways of accessing credit, offered by crowdfunding platforms;
- in investment services: high-frequency trading firms now account for a quarter of all volumes handled in the equity market. However, they enjoy a regulatory framework that allows them to operate without large amounts of capital, whereas banks are constrained by the requirement to have their own sizeable funds;
- in payment services, due to the emergence of TPPs, which PSD2 makes possible.

Even if we look only at PSD2, one might find it odd when considering the relationships which the Directive imposes. On the one hand, banks are forced to authorise access to their customers' account data while, on the other hand, TPPs are allowed to effect transfers within those accounts, which are the banks' responsibility.

Although the regulations fix some rules, they neglect to explain the framework. For example:

- while the regulations oblige the banks to set up ad hoc infrastructures to welcome these new service providers, there is, as yet, nothing in the texts *(either the Directive, or the RTS which are still being finalised)* which formally prohibits the use of "web scraping";
- in addition, the banks cannot insist on contractual relationships with the TPPs, nor can the banks prevent them from taking action, which makes any development of an economic model difficult.

Meanwhile, if the legislators wish the banks to remain the first person to turn to if there is a dispute, and that the banks should reimburse the customer if there is a problem with the TPP, then surely that means that the legislators consider, without saying so explicitly, that the banks are the most reliable party for the customer.

Nevertheless, the legislators have planned to ensure a minimum of security, and have asked the European Banking Authority *(EBA)* to define Regulatory Technical Standards, which aim to define the conditions of interaction between companies, in order to preserve the security of payment services.

At this stage, concerning exemptions from strong authentication such as those suggested by the EBA, we regret that a risk-based approach is not being taken, as this is both efficient and allows a precisely-targeted fight against fraud, thanks to proportional measures adapted to circumstances.

On top of this regulatory context, aimed at increasing the already-strong competition between banks, we also have the unprecedented technical revolution that digital progress has brought.

From a banking point of view, it is essential that the conjunction of these two phenomena doesn't erode customers' trust, nor threaten the security of money transfers, as trust and security make up the banks' number one asset! The protection of customers' personal data and their funds is a subject on which banks will never agree to compromise! That is why the regulations that apply to banks in their business activities must equally apply to the new companies *(GAFA and Fintechs)*. The security of the financial sector and end customers is at stake, as well as the need to respect the rules of competition.

Both innovative and secure, French banks are in a position to play a key role in developing the French financial sector's digital pathway, and in supporting a creative ecosystem with the Fintechs. They can do so in many different ways according to their own culture, their needs and those of their customers.

Banks and Fintechs develop together, each needing the other in order to grow, to understand what is at stake in the digital field and to assess properly the risks which both groups must face.

2. The new ecosystem which PSD2 will create

2.1. How the relationship between firms will change

PSD2 aims to oversee the new payment companies, as well as the ecosystem of payment institutions and banks.

> ***Clarification - Fintech:*** *a portmanteau word combining "finance" and "technology", these are innovative start-ups which use technology to rethink and offer financial and banking services at lower cost to the end customer. There are several categories of Fintech which exist: crowdfunding, virtual currencies, mobile apps, electronic payments, robot-advisors, etc.*

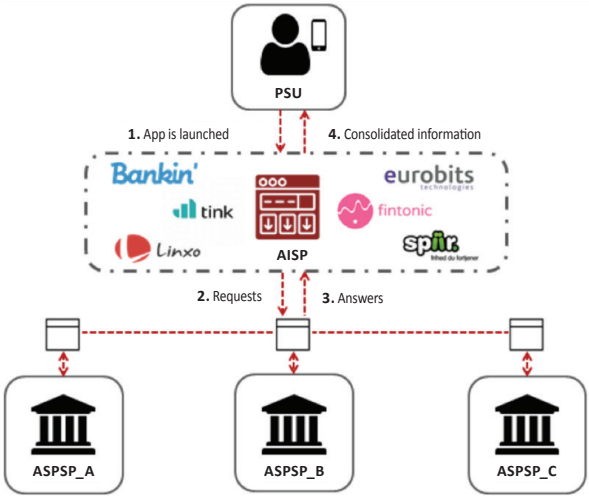
The market position of each of these types of companies, and the functions they carry out in the value chain of payments is outlined below.

2.1.1 The role of AISPs *(Account Information Service Providers)*

Les AISPs can offer their customers *(PSUs)* the opportunity to aggregate their various accounts held by different institutions *(ASPSPs)*, within a single app which can provide a consolidated view of their data.

The Directive provides for the following aggregation service: having obtained the prior consent of the customer, the aggregator will connect to the various ASPSPs which hold the customer *(PSU)* data, via a dedicated interface.

HOW AN AISP WILL OPERATE AS SPELLED OUT IN PSD2



Having recuperated the account information from each ASPSP, the app will analyse the data received and pass it on to a user-friendly interface that can present an aggregated overview of all the accounts.

Two aggregators currently dominate the market in France, **Linxo** and **Bankin'**. The former was set up in 2010, currently has 900,000 users and is the market challenger to the latter. **Bankin'**, is a Parisian Fintech which can claim 1.3 million users spread across four European countries. Another start-up which has made a name for itself in France is **Fiduceo**. However, this firm was bought out in 2015 by Boursorama, the online banking arm of Société Générale.

Around Europe, other aggregators have grown to a fairly large size. The most notable are **Tink** in Sweden, **Spiir** in Denmark and **Fintonic** and **Eurobits** in Spain, each of which can count about 350,000 users.

In order to stand out from the crowd, these platforms have developed other added-value services such as personal financial management *(analysing expenditure)*, or even document management *(bills, expenses claims, etc.)*. Customers are at the heart of these companies' strategies, with the aim of making their user experience as smooth and simple as possible via innovative and intuitive services.

INSERT 2 INTERVIEW

Joan Burkovic - *CEO of Bankin'*

***Galitt:** Could you present Bankin' to us?*

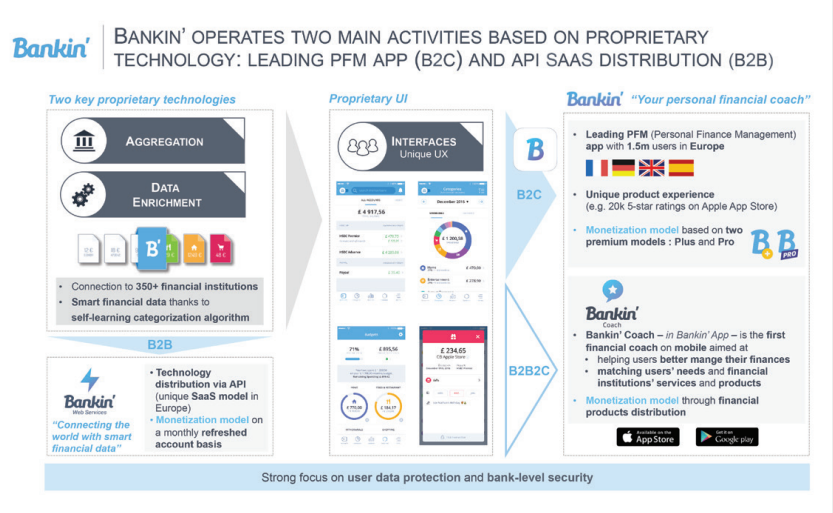
Joan Burkovic: Bankin' is an app which works like an intelligent financial and personal coach in order to help our users to manage their finances better from day to day. We're now present in four European countries: the UK, Germany, Spain and France and we have over 1.5 million users.

Aggregation technology has been developed by Bankin' so that we can connect our service to our customers' bank, or banks. This aggregation is essential for us to be able to offer our services, but it's not our main added value.

Our business model is three-pronged:

- **The first is a B2C or B2B2C model.** Here, the Bankin' app is a financial coach which enables our customers to manage their finances better and to receive personalised advice. In this way, if we see that a user has the opportunity to renegotiate a loan or to take out life insurance, we can suggest the idea to them, and even put them in touch with some independent specialised partners. We are the only totally independent company in the whole European market...

...Independence is the key to legitimacy amongst our users. We work with a wide range of partners *(insurance companies, banks, Fintechs etc.)* in order to offer our users the most relevant solutions possible. In this model, Bankin' is both a financial advisor and a business finder/ indicator.



- **The second business model is the one we offer via our Bankin' Web Services.** This is a B2B model, and we licence our API in a SaaS model. We offer our customers (banks, insurance companies, credit firms and others) the chance to take advantage of our aggregation technology and the smart handling of financial data. Our API allows our partners to respond to multiple cases. This API lets you connect to 350 different financial institutions in just a few clicks. We offer the SaaS model of our technology via a very easily-integrated Plug&Play API.
- **The third business model is the Bankin' Plus & Bankin' Pro model.** It allows our users to pair up the financial coach with extra features and services. For example, we've just developed an aggregation service for expense reports, in order to make life easier for our users who run up expenses while at work.

Galitt: *How do you think PSD2 will affect your business?*

Joan Burkovic: PSD2 is a great breath of fresh air into the market, as it establishes a legal framework for our business. This will also ease collaboration and increase the opportunities for innovation. In addition, it allows us to become both aggregators and payment initiators, which is very good news for our users.

Galitt: *What will the impact be for technical aspects?*

Joan Burkovic: Today, we use the "web scraping" technique and we are taking part in the development of the future technical standards, along with the EBA and the European Commission, within the framework of PSD2. This technique is a real advantage, as it allows us access to the same information as the customer. However, it does demand a lot of know-how in terms of development and maintenance.

We hear a lot of talk about APIs with PSD2. We have already worked with our banking partners via APIs. However, without real standardisation and harmonisation, APIs can be rather restrictive: Are they reliable? Will they take the load? Will they provide the same data? The idea of a universal API is very interesting, and one day we will get there in France and in Europe, but I doubt it will be in the short term. Bankin' is collaborating with the French and European regulators to help develop standardisation. If nothing comes of it, we will continue to use the "web scraping" technique.

As far as security is concerned, our app is audited very regularly by firms which are specialists in IT security. Moreover, in so far as we are working in partnership with banks, who are using our API in SaaS mode, we are regularly audited by banking companies. The real risk for banks today is the arrival of the GAFA. They have such financial power that they can innovate as and when they like. For Fintechs, the GAFA could be seen as an opportunity or as a threat. For the banks though, they are simply a threat. Without innovating themselves, they will have much to fear. The fundamental challenge is to always innovate in order to provide the best possible service to users.

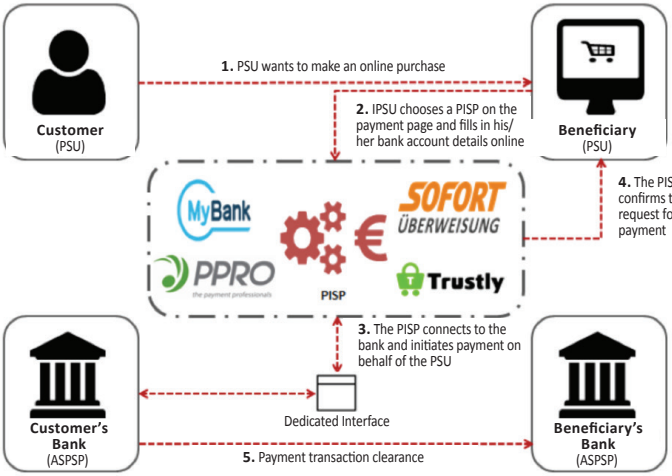
2.1.2 The role of PISPs *(Payment Initiation Service Providers)*

Those who initiate payment transactions are working in the field of e-commerce. These companies may initiate payment directly from the consumer's *(PSU's)* account. Thus, an e-merchant can broaden his/her payment portfolio by integrating these third parties alongside the big payment networks: **CB / Visa / MasterCard / American Express** or **PayPal**. When paying, a customer *(PSU)* could then choose to use a PISP to pay. The service claims to be simple, with no need for pre-registration prior to the transaction. The PSU will simply need to give authorisation for the PISP to have access to his/her account, by entering his/her online banking connection ID. This procedure will allow payment to be completed via transfer or withdrawal to the benefit of the e-merchant.

PISP's offers are mostly targeted at countries where the use of bank cards is less widespread. PISPs therefore have a well-established position in Northern Europe, particularly in Germany with **Sofort** *(a company from the Swedish **Klarna** group)*, and in Sweden with **Trustly**. Just as with the aggregators, these apps can be paired with other functions in order to offer more elaborate services.

Trustly can thus offer its customers a view of the balance in all their different accounts *(savings or current)* and enable them to choose which one to use for each payment. Its service today supports all the Swedish, Danish, Finnish and Spanish banks. **Trustly** is currently enlarging its network amongst games platforms and marketplaces, and also with money transfer services.

HOW A PISP WILL OPERATE AS SPELLED OUT IN PSD2
(FOR PAYMENTS MADE BY TRANSFER)



Ever since the setting up of **Sofort** in Germany in 2005, and the impact which its new online transfer service had, the European payments market has been in an unprecedented state, which continues today.

In Germany the banks, finding themselves unable to prevent **Sofort** from connecting to their interfaces, decided to ask the legislators to contest the legitimacy of this opening up of their interfaces and the access it gave to their customers' bank accounts.

At a European level, within the framework of the establishment of the Single European Payments Area *(SEPA)*, this new firm was seen by legislators, particularly the European Commission, as an innovator which can develop new, cheap and efficient payment services. In its PSD2 project the European Commission has therefore decided to favour this type of new service by proposing a regulatory framework which suits its development.

This is notable in its provision for data exchanges between third-party PSPs and ASPSPs, which will need to be carried out in accordance with new standards and communication protocols.

Since these third-party PSPs are already operating, as initiatives such as that from **Sofort** show, we will now describe their current modus operandi, known as "web scraping", as well as their future methods of working - Open APIs - along the lines set out by PSD2.

2.2. | From techniques of "web scraping"...

Currently, most AISPs and some PISPs use a technique known as "web scraping" or "web harvesting" in order to be able to function.

This "web scraping" technique is a way of extracting content from a website, via a script or a program which reads the html code, with the aim of transforming it, and being able to use it in a different context. It is a technique much used by, for example, price comparison websites *(trivago.fr, liligo.com, etc.)*.

In our example, a Third-Party Provider *(TPP)* will ask its customer *(PSU)* for his/her connection ID to his/her ASPSP (e.g. an online bank). It will then put this data into a program which acts like a robot, simulating the action of connecting in the customer's place. It can then harvest from the relevant page all the information it needs to operate.

2.2.*1* | How "web scraping" can pose several problems

- **For ASPSPs:** having a robot continually passing over your Internet page can slow the page down. If there are several simultaneous connections, this method can lead to what is called a "denial of service attack" *("DoS" - there are so many requests made at the same time that the server can't handle them all, leading to its crashing)*.
- **For TPPs:** this method requires them to have as many robots as there are ASPSPs, seeing as the different sites are not standardised, which leads to a very long programming time. The robots can also become obsolete overnight if an ASPSP decides to update or modify its page.
- **For the PSU:** when giving consent to a TPP, the PSU is giving access to all the information contained in his/her online bank account. Although the new services which are offered are legitimate, and the PSPs guarantee data confidentiality, they are nevertheless now capable of harvesting all the information in the customer account: balance, transfers, withdrawals, and the metadata associated with it *(time, date, place, business, amount, rent payments, refunds, loans, telephone operators, insurance, salary, medical insurance, consumer habits, etc.)*.

- **For all three parties:** the major problem with "web scraping" lies in the shared liability and the principle of proof. Let's take the example of a case of fraud, in which a transfer has been initiated from the account of a PSU without his/her knowledge. In as much as the PSU gave his/her online banking credentials to a TPP, it can be difficult to work out the chain of liability: does it reside with the PSU, the TPP or the ASPSP?

INSERT 3

PSD2's rules of liability

One of the stumbling blocks for PSD2 concerned the designation of liability between the various firms involved in each step of the payment chain.

Articles 73 and 90 have established rules of responsibility for Account Servicing Payment Service Providers *(ASPSPs)* to their users, in case of unauthorised, uncompleted or badly-completed payment operations, even though the payment operation is initiated by the Payment Initiation Service Provider *(PISP)*. The banks have condemned these rules of "strict liability" as going beyond general or common law. PSD2 includes, however, a number of guarantees:

1. An assumption of liability on the part of the PISP,
2. A first demand guarantee of reimbursement for ASPSPs against PISPs,
3. The right of ASPSPs to verify, in advance, that a PISP is satisfying the conditions laid down by PSD2,
4. And the transfer of the obligation to refund the PSU onto the shoulders of a PISP which is found to not be satisfying the conditions laid down by PSD2.

Nevertheless, the Directive doesn't require a contract to be signed between the two parties: a PISP may demand access to an account without a contract with the ASPSP. This point has been severely criticised, on the grounds that it would be preferable to guarantee the right of ASPSPs to contractualize their relationship with these third parties, under the auspices of prudential and banking authorities, such as the French ACPR.

Failing that, the rules of liability established by articles 73 and 90 of PSD2 could be in conflict with European Primary Law, and in particular with an ASPSP's fundamental rights to property and free enterprise, as well as a PSU's rights to privacy, such as they are outlined in articles 16, 17 and 7 of the European Charter of Fundamental Rights.

2.2.2 Data security at the centre of current concerns

As soon as you talk about the transmission of banking data, the question of security becomes essential. Today, protecting customer confidentiality and data integrity is central to banks' concerns. The European Banking Authority *(EBA)* has thus been made responsible, by the European Commission, for the setting up of specific measures aimed at limiting security risks.[3]

This step was initiated in December 2015, via the "Consultation Papers" *(sent to all stakeholders)* concerning strong authentication and communication security. This consultation work was completed in February 2016 with the creation of the Regulatory Technical Standards *(RTS)* documents. The latter were then re-submitted to all stakeholders via further "Discussion Papers" published by the EBA in August 2016, with all feedback received in October that year. Currently, all the information is back in the hands of the EBA, which has the task of compiling the opinions and validating its conclusions when it hands the final proposals for technical standards over to the European Commission. *(see also Timeline of Key Dates for PSD2)*.

2.2.3 The main conclusions of the EBA's work on technical standards

1. The process of authorisation for specific payment institutions:

The first measure is the requirement for all AISPs and PISPs to obtain certification as payment institutions from the relevant national authorities, so as to be able to study the reliability of the services being offered, primarily. There is a full process for PISPs and a lightened one for AISPs. In France the body which can carry out this certification is the Prudential Supervision and Resolution Authority *(ACPR - Autorité de Contrôle Prudentiel et de Résolution)*.

2. The use of certificates that conform to eIDAS[4] rules for both ASPSPs and TPPs:

eIDAS *(electronic IDentification And trust Services)* rules came into force on 1st July 2016. Their aim is "to create a climate of trust in the online environment" by providing a full, cross-sector, European framework for secure, simple and reliable electronic transactions between citizens and businesses. The EBA wants to rely on the use of eIDAS-compliant certificates to authenticate ASPSPs, AISPs and PISPs. However, January 2018, the planned date for transposition into individual member-states national law, may be too soon for the national authorities to be able to provide these certificates, as the certification infrastructure is still being developed.

3 - ***EBA*** *: Consultation Paper & Discussion Paper 11.2016*
4 - ***ANSSI*** *: EIDAS regulations*

3. The use of strong authentication:

In order to reduce the risk of fraud, and according to PSD2 guidelines, the EBA has imposed, via the Regulatory Technical Standards *(RTS)*, the use of strong authentication for third parties to be able to identify their customers. Therefore, every time the PSU consults, or makes a payment operation, he/she will need to be identified thoroughly, so as to be sure of his/her consent and intention to make that operation. In terms of information system security, this is called two-factor, or strong, authentication to describe a procedure that requires at least two authentication factors which can come from the following categories:

- What the PSU knows: a secret code *(e.g. a PIN);*
- Who the PSU is: biometrics *(e.g. fingerprints);*
- What the PSU owns: some form of authentication token.

The authentication procedure will remain completely at the discretion of the account managing ASPSP, but it could be carried out via the PISP if there is contractual agreement. Therefore, it is the bank *(ASPSP)* which will define the security procedures to be applied when a third party initiates a payment.

4. Exemptions from the use of strong authentication:

Aggregation will be exempt from strong authentication:

- as long as it isn't the first connection to the particular service, and that the current connection comes within a month of the previous authenticated connection;
- as long as the consultation is limited to that data which is classed as non-sensitive *(name and account number)*.

Payment initiation will be exempt from strong authentication for:

- contactless payment transactions of under €50, if the cumulative total doesn't exceed €150;
- remote electronic payment transactions of under €10, if the cumulative total doesn't exceed €100.

5. New standards and protocols for communication between firms:

In accordance with articles 97*(5)*, 66*(3)*b and 67*(2)*b of PSD2, ASPSPs must make a secure communication interface at the disposal of AISPs and PISPs, to share their customers' data. The EBA has left the technical implementation of this up to the firms involved, but has imposed the following conditions:

- There must be the same functions and availability as their online banking interfaces;

- There must be a guarantee of secure data exchange, via open and universal communication standards, thereby imposing the use of elements of the ISO 20022 standard which regulates exchanges of computerised data in the financial sector [5];
- There must not be the unaccompanied use of generic Internet standards such as HTTP, HTTPS, TLS and SSL which don't provide the necessary security guarantees for the exchange of financial data [6].

This access worries the banking sector as it sees in it a systemic risk for the financial system. They say the use of personalised security data *(authentication data or credentials)* by PISPs and AISPs resembles "handing the keys of your safe to a stranger", even though the access to the safe is limited both by time and to a single operation and is carried out "via secure and efficient channels". From a practical point of view, it should have been possible to allow the development of payment initiation and account information services without needing to hand over "the keys" to new companies which, as they hold them, are subject to lightened regulations concerning authorisation and prudential control *(very limited amounts of equity capital are required)*, and are particularly exposed to systemic risk of cyber-attacks.

It would have been technically possible for PISPs and AISPs to have access to payment accounts and to account data, respectively, without either knowing or using the identification data, by creating an API, as we will see later.

If a bank should refuse access to a payment account or to payment account data, other than via the use of an API, and this refusal is not based on objectively motivated and documented reasons connected to an unauthorised or fraudulent prior access, legislators will provide for a right of appeal in front of the ACPR on the grounds of "the need to preserve the security of personalised security data should not, however, prevent or complicate the use of AISPs or PISPs". Such an analysis, in our view, conforms to the principle of privacy by design, as set out in the new European regulations on personal data: giving access to the information needed for payment initiation and account information services is less dangerous for the protection of this personal data than giving a simple access to the bank account, while still allowing for the provision of these new services.

2.3. ...To the use of Application Programming Interfaces *(API)*

The idea of APIs had largely emerged even before the implementation of PSD2. Even though the text of the Directive doesn't mention the notion of APIs as such, and the EBA merely gives a list of technical requirements, APIs appear to be the most suitable solution, when taking all of those requirements, listed above, into account.

5 - ***ISO 20022*** *: Universal financial industry message scheme*
6 - ***Consultation Paper EBA*** *: 06.2016*

INSERT 4 INTERVIEW

Sébastien Taveau - *Chief Technologist at Early Warning*

In order to shine further light onto the ideas of APIs and Open APIs, we spoke to Sébastien Taveau, Technologist at Early Warning.

Galitt: *Could you define what the term "API" means for you?*

Sébastien TAVEAU: An API is a structured means to open a service or some data to third parties via an easily-controllable and secure gateway. In essence, it is no more or less than a logic of questions and answers.

Thus, in the example of a data aggregator *(AISP)*, he will send a request from his application, asking to recover defined data. This request will be handled via the gateway, the API, which will ask the relevant part of the ASPSP in order to get hold of the information. The data will pass via the gateway to the AISPs application, which will compile it. *(see graphic p.16)*.

HOW AN API WORKS

Galitt: *What is meant by the term Open API?*

Sébastien TAVEAU: There are several types of API, of which the main ones are:

- **Private APIs:** This is a 1:1 integration. In this case, the API has been conceived with a specific partner in mind, and is usable only by them. Private APIs are very generally used for sharing sensitive data, which can pose dangers for those involved *(black lists, personal data, etc.)*.
- **Public APIs:** These are the most widespread APIs, and don't pose any particular concerns. We could give the example of Google Maps' API or that of Twitter's news feeds. Registration is encouraged but not necessary.
- **Open APIs:** These are conceived for a wider public than Private APIs. They require a third-party PSP to accept the terms and conditions of use, and necessitate a guarantee and security procedure via the authentication enrolment called "OAuth". Registration is required for this service. Within the framework set out by PSD2, Open APIs are the ones which best correspond to the need to use dedicated interfaces, as Open APIs allow an ASPSP to verify the users which connect to their service wanting to recover data.

Another important element to take note of is that some APIs can generate revenue, whereas others don't bring high added value *(used for broadcasting free media content or as an eye-catching service, but without any particular economic outlook)*. For example, Public APIs are not aimed at turning a profit, but it is important to mention the maintenance costs and the data input, as all types of APIs have a significant financial impact. The business model lies in the large-scale use of APIs, or the cross-pollination with other APIs, or via the underlying paid services that come with the use of an API. It's possible to bring together several different functions, depending on the mapping capacity of the APIs.

Galitt: *What advantages can Open APIs bring?*

Sébastien TAVEAU: APIs, and particularly Open APIs, offer a lot of flexibility as they allow you to keep a layer of security, while forcing the administrator to think about what uses might be required by third parties. I often compare an Open API to an object inside a box made of toughened glass: you can see it, you can shake the box, but you can't touch it.

As we have seen, an API is a group of predefined calls which access a service via a gateway. The gateway is the critical point, in terms of security, as the third-party PSP will, via the API, directly connect to the ASPSP's information system. Technically, it is easy to build into the system a way of locking down the communication if a problem is detected. Moreover, with an Open API, the OAuth authentication is mandatory, which further reduces the risk. OAuth is not an authentication protocol, but a protocol to delegate authorisation, so it can authorise an application to use a secure API on behalf of a user. This represents an added layer of security, on top of that brought by the strong authentication. Once again, the analogy of the object behind toughened glass is very striking. In addition, the reply provided by the API is the only information that the TPP can receive, which is essential."

To summarise this section, we can see that the directive will completely revolutionise relationships between companies, both legally and technically.

The biggest impact of these innovations today will be felt by the banks themselves. In the next section we will analyse the different possibilities offered at the moment, and the noticeable initiatives.

3. A strategic turning point for the banking sector

3.1. Three potential business models

What is principally at stake for the banks today is the need to find the appropriate positioning relative to all this innovation.

According to a survey by Finextra in 2015, 88% of European banks are still preoccupied by security risks.[7] They are equally uncertain about what format of communication interface and security protocols to set up. A major risk for the banks is the possibility that use of bank cards will fall, in favour of the services offered by PISPs. This is why banks need, as of now, to look to reform their business models, in order to protect their customer relations and the profitability of their payment services.

The banks seem to be aware of the need to act on these points. The same Finextra survey found that 54% of European banks say they are currently rethinking their customer relations model and other associated business models.

3.1.1 | Three business models types stand out

Internal Model:

The Internal Model involves the bank using its internal resources *(strategy and R&D departments)* to provide innovation. The advantage of this business model is that the bank keeps control of all the channels of interaction with the customer at the bank's disposal *(apps, payment terminals, cards, etc.)*. The drawback is that, in order for it to work, the bank needs a lot of resources, both human, technical and financial, to be able to react to a very competitive market and to offer innovative services.

Hybrid Model:

In this model, the bank relies directly on the ecosystem of Fintechs or third-party PSPs. The aim is to take advantage of the know-how and technical abilities of these new firms in order to quickly be able to offer services of interest to customers. The challenge for the bank is to take control of these innovations via acquisitions or setting up joint ventures. In this model the Fintechs play the role of R&D laboratory, which can be absorbed by the bank. It also helps the bank to limit its need for internal resources, and to react quickly.

Disruptive Model:

The disruptive model activates Open-Banking's modus operandi. The bank allows other companies access to its back office via Open APIs. The bank's priority is...

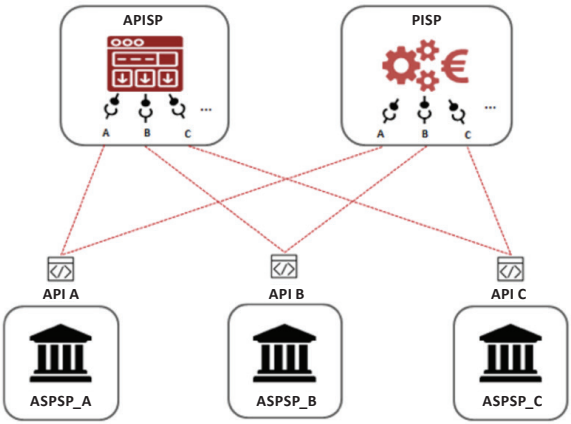
7 - ***Finextra***: *PSD2 and XS2A - Regulation or Opportunity?*

...to emphasise its role as a safe for customer information, and offers a complete range of solutions via third-party applications. There is one large stumbling block with this model, however, which is standardisation *(see diagram below)*. Without accepted standards and a strong desire for them on the part of governments, these technical implications appear sufficient to make this model too uncertain. Finally, the major risk is that of disruption bringing a third-party provider to a dominant position over one or more of these services.

3.1.2 The standardisation of APIs, essential for the disruptive model

Standardisation is a fundamental part of the deployment of the disruptive model. For it to work, the TPP must be able to connect via a secure interface, essentially an API provided by the ASPSP, and recover the information it needs.
The diagram below shows how APIs are set up by ASPSPs on behalf of TPPs.

DIFFERENT APIs FOR EACH ASPSP



The diagram shows that in order to connect to bank A, the TPPs *(AISPs or PISPs)* have to identify the technical means to allow their apps to connect to the particular bank's API and to interpret the data received. This development operation has to be repeated for each different ASPSP. The TPPs therefore need to be able to handle the technical complexities stemming from a great variety of API programming and tiered data.

These were the findings of the **Open Bank Project**[8], set up in 2012 by the German firm **Tesobe** in order to begin the work needed to create a universal API for the banking sector.

OPENBANKPROJECT

8 - ***OpenBankProject***

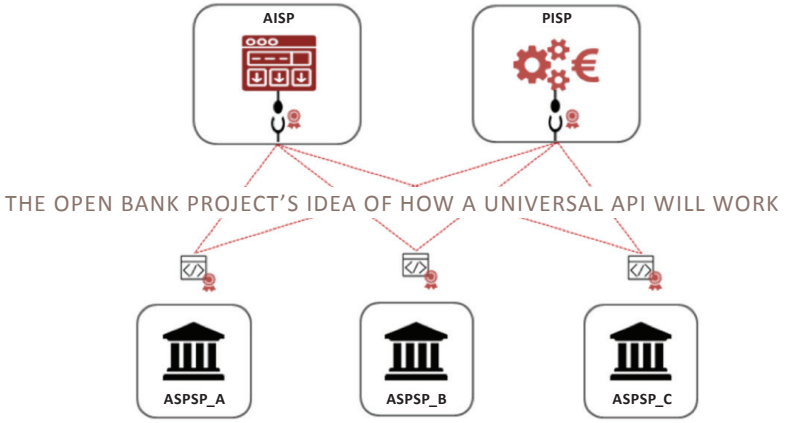
Aims: to create a project for an Open Source API for banks, so that the whole banking ecosystem can work in an intelligent manner and usher in the era of Open-Banking. The principles of standardisation and universality are the foundation stones.

To achieve this, the Open Bank Project, the think tank of Open API, carried out a huge survey of the banking ecosystem, to find out what all concerned expected from it. The Open Source project has so far brought together over 5,000 developers, aiming to provide an API catalogue, an environment for secure tests and a panel of experts at the disposal of anybody with questions.

"We're providing a standard, a data model, a platform that banks can use internally, and access to the global community of developers and Fintechs. It's a way to move away from the rigid, closed architecture towards the web standards which are simple to use and accessible to a huge number of developers. When a bank allows others the opportunity to build on the bank's own services, they are able to transform themselves into a platform distributing all sorts of apps via their own "app store"".

Ismail Chaib, COO of Tesobe / Open Bank Project[9]

The Open Bank Project's vision is outlined in the following diagram:



In this diagram the TPPs and the ASPSPs use the same communication standards. Thus, each API is identical and only one type of program is needed. Standardisation makes inter-company relations easier. Looking further ahead, the project aims to clear the way for Open-Banking. Banks will become a modular platform upon which firms can interact via the API.

This principle of bank-as-platform, is outlined in the case study of **SolarisBank** on the following page.

*9 - **AGEFI** : APIs bringing innovation to banks - LINK*

INSERT 5

SolarisBank, the bank of tomorrow?

SolarisBank was founded in 2015 by the German financial group **FinLeap**. It claims to be the first 100% digital bank, and received its banking licence from the German financial regulator, BAfin, to be authorised to operate in accordance with existing regulations.

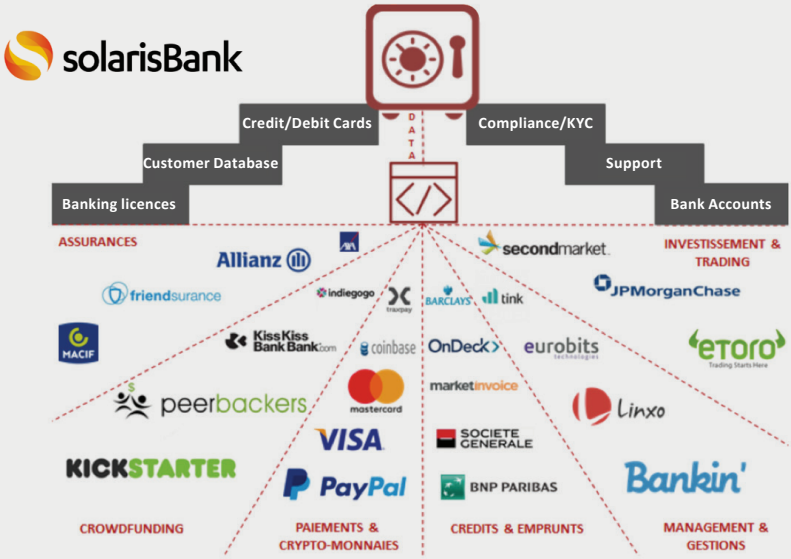
Targeting its strategy at young businesses, **SolarisBank** operates a B2B2C business model which is typical of Open-Banking. It offers a white-label platform by which banking services can be provided à la carte by whichever Fintechs want to work with it. Customers can then interact directly to create the banking environment they prefer by choosing the apps they want.

The bank thus serves as a modular toolkit via its API.

"Our services are like Lego bricks: our partners can choose the bricks that they want and assemble personalised solutions with them to meet their own needs. Partners can get access to the Solaris Platform services through our API. Integration is simple and allows users to concentrate on their own roles. In addition, our services are secure and guarantee the confidentiality of our user data."...

Andreas Bittner, Managing Director SolarisBank [10]

OPENBANKING'S ILLUSTRATION



10 - ***SolarisBank*** : *Presentation*

... In addition, **SolarisBank** acts in a modular fashion across several APIs. There is a sense of interoperability between the different companies represented. In short, a firm can use this white-label platform in order to create its own bank. **SolarisBank** retains the key banking functions, such as customer database, card issuing, bank account management, compliance, risk management etc. Nevertheless, it brings in different companies for the implementation of each step.

In this bank-as-platform model, the banks position themselves at the centre of a new economy in which APIs are a source of income and allow the banks to meet the various needs of their customers more efficiently.

SolarisBank is not the first company to offer this type of model. The pioneer in this field is **Fidor Bank**, recently acquired by the BPCE group.

3.2. The British model: an early implementation of the Directive?

The United Kingdom is a key strategic market for this sector, as the British government has taken a clear position in favour of APIs, of standardisation and of Open-Banking more generally.
In 2015, Her Majesty's Government, via its Competition and Markets Authority *(CMA)*, launched a study of the personal banking market [11]. The results of this undertaking showed that traditional banks had a lot of trouble innovating, and that Fintechs were being slowed down in their innovation by their lack of access to customers' banking data. Moreover, this study revealed how customers, mainly small and medium-sized businesses *(SMEs)*, wanted to have access to information held by their banks in order to make their everyday business easier, particularly when it came to sending out invoices. They were attracted to the possibility of opening up their data to third parties, so as to receive investment advice more quickly and simply, but also to be able to carry out bank transactions to customers without fuss. Therefore, even before PSD2, the British authorities decided to take this approach further.

Thus, in September 2016, the Treasury Department decided to set up the *Open Banking Working Group* [12]. This working group brought together banks, other businesses in the sector, consumer associations, research institutes and, especially, the Open Bank Project. Its objective was to make the country the pioneering land for Open-Banking.

*11 - **CMA** : Retail banking market investigation*
*12 - **Open Banking Working Group***

The group has since based its work on the themes of the *Open Banking Standard*[13], in order to decide the structure needed for the APIs, their development and maintenance, but also to define the standards of the data that is one to be transferred. In addition, the *Open Banking Working Group* is working on appointing a governing body, a body of reference in charge of setting things up.

Finally, it was decided that British banks should adopt a common digital standard before 13th January 2018 - the final date of PSD2's transposition across the European Union. Thus, the British authorities decided that the digital norm to be used will be that for APIs. At this point in time, the project is ongoing and seems to be working constructively between all parties.

The stance held by the British legislators is important, as it could influence the European market. The country, which is a reference point for Fintechs and currently a global financial centre, hopes to hang onto its leading position. It has anticipated the advantages that this could bring, enabling it to become a reference in the sector if it comes off.

"The United Kingdom has the potential to be a world leader in data handling to help competition and stimulate innovation in the banking sector, which will give customers more choice and help them to save money."

Anthony Browne President of the British Bankers Association *(BBA)*[14]

The uncertainty around this initiative is focussed on the level of harmonisation concerning all the interfaces, with the potential risk of having to duplicate new infrastructures in parallel. Currently, the British government claims not to be working independently - "in a silo mode" - but rather in partnership with European legislators, so as to avoid this risk.

Two questions arise: Could the UK anticipate the Directive's transposition by testing the development of a standard for APIs? Or, on the other hand, will recent moves towards Brexit mean a greater desire for the government to differentiate itself from Europe and be proactive about regulation and standards?

3.3. Existing French initiatives

In France various initiatives have been taken by the banks on this subject. As mentioned in Insert 5, on the subject of **SolarisBank**, **BPCE** group announced the purchase of **Fidor Bank** in July 2016[15]. This move is in line with the group's declared strategy of "Growing Differently". The aim is clear: strengthen and accentuate the bank's digital transformation.

*13 - **Open banking Standard***
*14 - **Finextra** : UK sets out open banking API framework*
*15 - **Groupe BPCE** : communiqué de presse sur l'acquisition de Fidor Bank*

Fidor Bank was set up in Munich in 2009 and was the first totally digital neo-bank. As with **SolarisBank**, its strategy marks a clean break from competitors and Open-Banking is a priority. The arrival of a major shareholder in **Fidor Bank's** capital gives it the means to follow and accelerate an offensive strategy, aimed firmly at innovation and customer service. In fact this bank is targeted at individual customers, unlike **SolarisBank** which focusses mainly on professionals. **Fidor Bank** relies on a community of 350,000 members, of whom 125,000 are customers, who are encouraged to get involved in the bank's strategy by helping to define its supplementary services, or suggesting changes to its existing ones. The community, like a social network, shares its advice, including advice about offers from rival banks. Active members are rewarded for their involvement.

As for the analysis of business models, BPCE group stands out for its policy of diversification, in as much as it has opted for a hybrid model which consists of acquiring a start-up that follows a model based on disruption and Open-Banking. The hybrid model is the one which currently appears to be the most popular amongst French banks.

Thus, **HSBC France** began a partnership with **Linxo** in October 2016, so as to offer its customers the latter firm's technology and services under a white-label [16], thereby giving them the chance to receive help in the management of their personal finances.

Société Générale group, via its retail bank **Crédit du Nord**, has launched its service aggregator, called "Synthèse multi-banque", based around technology developed by **Fiduceo**. The stated aim is to offer customers an aggregation system for their accounts initially, developing later to encompass producing invoices. Société Générale has also announced that it is currently working on its account aggregation app, which will equally use **Fiduceo** technology. [17]

Crédit Agricole has spent several years developing its own API so as to be able to collaborate with developers. This API, called "Simone" was born in 2012, thus allowing developers to supplement the features of its banking app. The principle is simple: the bank provides a software development kit via this API that gives developers secure access to its customers' banking data. The bank has gone further along this path and anticipated the danger of data theft, by accepting complete legal responsibility in case of fraud or theft. It is important to note that this initiative is a world first.

*16 - **Linxo** : press release about its partnership with HSBC France*
*17 - **Capital** : Société générale et crédit du Nord*

The bank then created its own app store, called the "CAstore", allowing developers, whom they called "Digiculteurs" *(or "Digiculturalists")* to offer their apps to the bank's customers. They have set up an innovative economic model [18]. Customers who use between 1 and 10 apps per month pay a flat rate, and the sums earned are used for the upkeep of the platform, with the money left over going to the developers.

The platform has been very successful and Crédit Agricole organises regular hackathons in order to stimulate further innovations through themed competitions. Examples included the Mobile Banking Factory in May 2015 [19], or a January 2016 competition based on connected habitats [20].

We should also take note that the apps which have been developed are not all aimed at the banking sector. The goal is often to be able to offer innovative services to business customers that work via their data. This is why the bank invested in **Linxo** in January 2016 [21]. The bank is to begin this service, following a test amongst **BforBank** customers in 2017. The app will be rolled out to all of its branches if the test is successful.

*18 - **Finextra** : UK sets out open banking API framework*
*19 - **Crédit Agricole** : Challenge Mobile Banking Factory*
*20 - **Crédit Agricole** : Habitat Connecté*
*21 - **Linxo** : communiqué de presse sur l'entrée au capital du Crédit Agricole*

In conclusion, it appears that French banks are favouring a hybrid business model at the moment. This allows them to take advantage of the technology provided by the aggregators while keeping control both of their image and of their customer relations.

INSERT 6

Will banks be liable for their app stores?

What would happen if one of these apps contravened the law? Would a bank be liable for an illegal app developed by a third party but released via its own app store?

For France, the answer is contained in the law for trust in the digital economy, dated 21st June, 2004[22] *(LCEN – Loi pour la Confiance dans l'Economie Numérique)*, which applies to all public communications, including app stores provided by banks.

LCEN distinguishes between two types of company: content editors, which are automatically liable; and hosts, which only become liable if they do not act promptly to remove all illicit content, once they have been informed of its illicit nature. When applying LCEN, the bank can be considered as editors of apps only if it validates the app before making it available to the public. Otherwise, the bank can only legally be considered as the host of the app.

3.4 Third parties, outside the banking sector, eyeing up banking data

Three profiles exist for third-party companies which are closely interested in banking data.

Firstly, we have insurance firms, which look on PSD2 as a chance to become payment institutions, and to offer their mutualist members the chance to bring all their accounts under one roof. In France, **MAIF** has recently launched just such a bank account aggregation service, called "Nestor", developed under a white label using technology from **Linxo**.

"Digitalisation involves a general lowering of entry barriers. Working from this analysis, we are very defensive of our core business, but there's nothing stopping us from having an offensive approach to other branches of business."
Pascal Demurger, Managing Director of MAIF. [23]

22 - ***Legifrance*** : *Law n°2004-575 dated 21st June 2005 for trust in the digital economy*
23 - ***La MAIF***

The second group are mobile telephone operators. As an example, the launch of Orange Bank, scheduled for 2017, shows the company's desire to offer banking services to its customers. What is more, **Orange** has acquired a majority stake in **Groupama Banque**. Its objective: 2 million customers in the long term.

Finally, the last, and most disturbing, group is the GAFA *(Google, Apple, Facebook and Amazon)*. These web giants which are at the heart of data management, and of what is more widely known as Big Data, have asserted their ambition of shaking up the traditional banking firms. Their entrance into this new market shows their desire to get hold of any and all types of data in order to have an ever-deeper knowledge of their users. We should mention the examples of **Google's** price comparison tool, launched in 2016, and **Apple Pay** in 2015, or **Facebook's** Messenger Payments in the same year. Amazon has also taken the leap by opening a credit arm, with **Amazon** Lending, launched in 2012 and the Amazon Store Card in 2015. The stakes for each are huge: being in charge of the entire value chain and making the customer path more fluid, but particularly intensifying their core business of data collection and thereby getting to know their users and their users' habits even better. For the moment the firms are discreet, but nobody needs reminding of their financial muscle which would allow them to easily swallow up the Fintechs which are currently trying to position themselves on the front line of PSD2. Opportunity or threat? The question is there to be answered, and PSD2 is leading us to a new era in banking.

Conclusion

Are we at the dawn of an era of Open bank data?

PSD2 is another step along this path, begun in France by the banking mobility service *(planned by the Hamon- and Macron-sponsored bills)* and more recently by the law dated 7th October 2016 for a digital republic. This latter bill enshrines data portability in law and entitles consumers to recover their data from their digital service providers in order to transfer them to another service provider. The law complements laws of data portability anticipated by the European general protection of data regulations of 27th April 2016. Banks find themselves within the scope of this text.

On the contrary, the boom in the banks' online services has made this sector a key target for the new regulations which are essentially aimed at opening up the market to new firms in order for consumers to get the benefits, just like PSD2. As of 25th May 2018, this data portability law will allow consumers *(particularly of online banking services)* to recover, with a single request, all of his/her files and consumption data. To be able to do this, online service providers will have to take all the necessary measures for a change of provider, particularly in terms of programming interfaces and data transmission. So, we come back once again to the subject of APIs...

All through this white paper, APIs and in particular Open APIs, stand out as a real alternative to web-scraping, and a pivotal point between security and innovation. Nevertheless, there is still a long road left to travel to reach standardisation of APIs and data structure, thereby allowing full interoperability between services in this new ecosystem.

We can note that French banks, after having initially been reticent, have understood what is at stake and are taking the opportunity to develop projects in this area. They were inspired by German banks such as **SolarisBank** and **Fidor Bank**, which led the way in Europe for Open-Banking.

But how far can this movement go? As far as normalising banking data, which has until now been protected by traditions of secrecy and security?

In any case, it is vital that the banking sector watches current developments very closely. Instead of suffering the blows landed by new firms which are often more agile and less heavily-regulated, banks could seize the bull by the horns by putting themselves at the centre of the action, with a responsible and balanced definition of conditions for access to bank accounts. And by creating the conditions for a new ecosystem that creates value for themselves.

ABOUT THE AUTHORS

Thibault Verbiest
De Gaulle Fleurance & Associés

A lawyer and a former businessman, Thibault Verbiest boasts thorough experience particularly of intellectual property, but also of the sectors of technology, the media and telecommunications.

He advises firm's clients in a variety of operations, from the dematerialisation of banking and financial services, to the digital transformation of companies, and including mergers and acquisitions in the technology sector. He also assists clients on certain litigation files, especially in the fields of intellectual property or liability connected to cybersecurity.

Several other colleagues from the law firm of De Gaulle Fleurance & Associés have assisted on this project:

Jonathan Souffir: Partner

Jean-Sébastien Mariez: Senior Counsel Lawyer

Hermien Van Der Vynckt: Jurist

Paul Noel
Galitt - Payment Consulting

A graduate of the Ecole de Guerre Economique (EGE), Paul Noel is currently Consultant within Galitt's Payment Consulting Business Unit.

Several colleagues within Galitt have assisted with this project:

Hervé Ammeux: Practice Director

Emmanuel Caron: Practice Manager

Benjamin Deblauwe: Project Manager

Gérard de Moura: Managing Director

Stéphane Dubois: Practice Manager

Jérémie Fave: Payment Consultant

François Flouriot: Practice Manager

Vincent Mesnier: Executive Vice-President - Testing Solutions

Anne-Sophie Mouraud: Payment Consultant

Isabelle Pujadas: Communication Director

Gérard Tchakgarian: President

Diane Walch: Business Development Director

Galitt

17 route de la Reine
92100 Boulogne-Billancourt - France
Tel. : +33 1 77 70 28 00
contact@galitt.com
www.galitt.com

DE GAULLE
FLEURANCE
& ASSOCIÉS

SOCIÉTÉ D'AVOCATS

9 Rue Boissy d'Anglas
75008 Paris - France
Tel. : +33 1 56 64 00 00
www.degaullefleurance.com

Graphic design : www.jean-charles-dart.weonea.com