Account aggregators and payment initiators, providing fresh impetus for banks

Rémi Steiner
Conseil général de l'Économie

[special issue of *Réalités Industrielles*, February 2019]

Abstract:
A large share of Fintech companies are active in the field of payment services. The European Commission has taken note of their expansion, driven both by the immediate interest of consumers in cheaper and more innovative financial services and by the belief that the harmonisation of payment services is a prerequisite to the creation of a digital single market.
Authorities in the UK have given their citizens the ability to easily make their banking data, held by major UK banks, available to third party financial service providers. The spread of this practice (known as open banking) in Europe is currently the subject of a fierce battle, the outcome of which may significantly curtail the supply of banking services and weaken links between consumers and traditional banks.

New payment services and new regulated stakeholders emerge

European harmonisation of payment services

Until a decade ago, the legal framework applicable in the European Union to payment services was splintered into twenty-seven separate systems. In France, for example, only credit institutions were allowed to make means of payment available to their customers, while other European countries took a much more liberal approach.[1]

In the European Commission's view, harmonisation of the single market for payment services is an essential condition for the completion of the internal market and the free movement of goods, persons, services and capital. An initial step towards harmonisation was behind Directive 2007/64/EC of 13 November 2007 on payment services in the internal market, known as the Payment Services Directive (PSD).

The initial PSD brought together widely varying national traditions: it dismantled banking monopolies where they existed. It introduced oversight of stakeholders that, in other jurisdictions, had previously been unregulated. It established up a list of payment services. It created the status of "payment institution" – institutions that are authorised to provide payment services alongside banks, subject to approval from the banking supervisory authorities, but that are subject to reduced prudential requirements, in particular as regards the level of equity capital required.

[1] Nevertheless, barriers to regulatory entry have not always been associated with higher prices or lower quality of the financial services on offer.

Account aggregation and payment initiation: the trailblazers

The Payment Services Directive heralded the arrival of a number of Fintech companies, which gradually made their way into the Malthusian world of financial services. Some offer payment services which had escaped the notice of the drafters of the first Directive and had therefore not been identified as such; these were able to continue to expand outside the payment institution status.

These include Sofort GmbH, the best example of what is now known as the "payment initiator". Since 2005, Sofort has offered *Sofortuberweisungen* (immediate bank transfers), a paperless payment procedure that is independent of banks. It is a widely used online payment method in Germany, Austria, Switzerland and Belgium.

When it is time to settle a purchase, the merchant site offers the consumer the possibility to switch to Sofort's payment application. The customer chooses the bank and account she wants to debit and enters her bank details (which are not retained by Sofort). The application connects to the customer's online banking site in her stead, ensures that there are sufficient funds, orders the transfer expected by the merchant on the customer's behalf, and then provides the merchant with the completed transaction's characteristics (including the reference number that allows the merchant to reconcile purchase and payment). Compared to a credit card transaction, Sofort is inexpensive for the online merchant; the method is fast, secure and easy.

Account aggregators have also escaped the net of the first PSD. Following the example of the French Fintechs Bankin and Linxo, account aggregators offer consumers who have agreed to hand over their bank details consolidated, regularly-updated views of their bank accounts.

Like payment initiators, account aggregators access online banking sites using the identity of the customer who has authorised them to do so. They read, interpret and record banking transactions. Services that banks had refrained from offering, such as automatic categorisation of expenses, online access to multi-year histories and analysis of recurring flows, allow aggregators to offer high value-added services, including period-to-period comparison of revenues and expenses, announcement of upcoming banking transactions, and predictable changes in account balances.

Security issues and pushback from banks

The growth of these new services clearly involves risks. One of the most acute is the existence of databases of bank identifiers at account aggregators. Hacking them would be of great interest to fraudsters – identifiers not only provide access to accounts, but also, generally speaking, allow transfers to be issued. A criminal with these codes could quickly appropriate the assets of a large number of customers. The stolen sums could be quickly scattered and therefore difficult to recover.

If, as payment originators and account aggregators wish (hereinafter jointly referred to as "third party providers"), consumers became accustomed to using their bank identifiers outside their online banking site, they could be more easily misled. They could be less reluctant to provide their bank identifiers on a website that appeared to be a financial services provider, but which existed only to swindle them.

Fearing that in such cases their liability would be called into question, banks have sought to contractually protect themselves: the general terms and conditions governing the management of remote accounts usually include a clause prohibiting customers from disclosing their login details. For liability reasons, and also to defend their interests, banks have tried by all means to hamper the growth of these new service providers.

In response to legal proceedings brought against Sofort by Giropay GmbH (founded by Postbank, German savings banks and cooperative banks), for the purpose of preventing Sofort from offering online credit transfer services, Sofort filed an appeal with the German competition authorities (the *Bundeskartellamt*) on 15 July 2010. This appeal was decisive for the future of the sector and with respect to Community regulation.

Following its investigation and under the terms of a ruling handed down of 5 July 2016,[2] the *Bundeskartellamt* considered that the general terms and conditions of German banks, without the security issues invoked being sufficient to justify it, restricted competition between the different providers of payment services in the Internet, violated German and European competition law and ultimately hindered the offer of new and innovative services in the growing market for payment services in the e-commerce sector.

Legitimization of third party providers by the Second Payment Services Directive

In line with the *Bundeskartellamt*'s then-pending ruling, Directive 2015/2366 of 25 November 2015 corrected the shortcomings of its predecessor, the First Payment Services Directive, and included specific provisions for account aggregators and payment originators. The new Directive entered into force on 13 January 2018.

Like the first PSD, the second Directive opens the market to competition from new entrants,[3] while including them within the scope of supervision, albeit in a lighter way. Account aggregation and payment initiation services are now part of the list of payment services. Account-keeping institutions[4] may not object to their customers providing these third party providers with access to their payment accounts, even in the absence of contractual relations between the account-keeping institution and the third party provider concerned.

In return for this freedom of access, payment originators are now subject to approval, and account aggregators are required to register themselves. They are also required to take out civil and professional liability insurance covering the risk of unauthorised or fraudulent access to or inappropriate use of payment account data.

Finally, relationships between account-keeping institutions, account aggregators and payment originators must be based on "common and secure open standards of communication" and are subject to a requirement to implement security measures. These standards and security measures have been included in a delegated regulation,[5] prepared by the European Commission on the basis of a draft text from the European Banking Authority (EBA). Delegated Regulation 2018/389 of 27 November 2017 (which was only published on 13 March 2018) will only come into force on 14 September 2019.

---

[2] See the ruling of 29 June 2016 by the Bundeskartellamt, "Beschluss der Spitzenverbände der deutschen Kreditwirtschaft; Sorgfaltspflichten in den Sonderbedingungen für das Online-Banking",
https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/AktuelleMeldungen/2016/29_06_2016_Ver%C3%B6ffentlichung_Entscheidung_Bezahlverfahren_im_Internet.html

[3] See "Commission Staff Working Document: Impact Assessment Accompanying the Document "Proposal for a Directive on Payment Services in the Internal Market and proposal for a Regulation on Interchange Fees for Card-Based Payment Transactions", Brussels, 24 July 2013, SWD(2013) 288 final, Volumes 1/2 et 2/2

[4] For the remainder of this article, credit or payment institutions are referred to as "account-keeping institutions" or, for ease of use, as "banking institutions" or "banks".

[5] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.

The difficult implementation of a new framework

Problems with establishing technical standards

How can a third party provider, whether an account aggregator or a payment initiator, be allowed to insert itself between a consumer and an account-holding institution, by guaranteeing transaction security, data confidentiality, a clear sharing of responsibilities and the ease of use that has made third party providers so successful? The issue is a thorny one. It has given rise to bitter disputes, both prior to the drafting of the Second Directive and after its publication, when it came time for a precise agreement on technical standards for authentication and communication.[6]

At the heart of the discussions is the question of the future legality of webscraping, which is currently deployed by account aggregators with the consent of their customers. Webscraping is a technique that allows a robot to identify itself on an online banking site as if it were the account holder itself, to read and interpret the information displayed (account balance, transaction titles, etc.), and then to return this information to the customer in a new and enhanced form with services.

Aggregators, like payment initiators, have developed a plethora of interfaces that allow them to extract account information that is accessible on the remote banking sites of any banking institution. These tools keep aggregators separate from banks, with which they do not need to sign agreements. The flip side is the requirement and the responsibility for aggregators to keep their customers' login credentials secure, as this data is particular sensitive.

One can imagine the frustration of banks, which considered their customers' account statements as a valuable asset entrusted to their keeping, and which – noting that a growing proportion of online banking consultation flows are repetitive and concern large batches of customers – may rightly worry that certain queries or payment orders are of fraudulent origin, and which may fear that one day they will be called to account for a lack of vigilance.

The idea of a dedicated channel for exchanges between banks and third party providers

The solution by EU legislators consists in requiring account-keeping institutions to have a communication channel reserved for third party providers: any payment account manager with an online banking service must also offer account aggregators and payment originators a dedicated interface.[7] In this way, consumers can identify themselves to their third party provider, and third party providers can identify themselves to banks, without using the identifiers that consumers use in their direct relationships with their banks.

Although this solution is attractive, the devil is in the details. Account aggregators and payment initiators have only been able to expand – to the detriment of banks – because they have often been more attentive than banks to their shared customers' needs, and more skillful in launching IT projects. Can we hope that they will make the implementation and quality of their services dependent on banks' goodwill and diligence?

---

[6] In this respect, see the draft regulation drawn up on 23 February 2017 by the European Banking Authority (EBA), Draft Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication under Article 98 of Directive 2015/2366 (PSD2)", as well as subsequent exchanges which this project generated with the Commission (www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2)
and the discrepancies between the EBA's draft and the text of Regulation 2018/389 of 27 November 2017.

[7] See Article 30 of Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.

European legislators, who do not wish to hamper these stakeholders, has instituted guarantees in their favour. Banks are required to justify that their dedicated third-party interfaces have, at all times, the same level of availability and performance as those intended for their customers. To mitigate the consequences of a failure, banks are asked to provide a backup communication channel[8] with the third party provider. Account aggregators and payment initiators must be able to test the interfaces six months before they are launched, i.e. as from 14 March 2019 for interfaces intended to be operational when Regulation 2018/389 enters into force.

The development of Application Programming Interfaces (APIs)

Several national groups[9] have launched (conflicting) efforts to specify the communication interfaces (Application Programming Interfaces, or APIs) used between account-keeping institutions and third party providers. In addition, a European working group, the Application Programming Interface Evaluation Group,[10] brings together representatives of all stakeholders: consumers, account holders and third party providers, in the presence of representatives of the European Commission, the European Central Bank[11] and the European Banking Authority.

It is not certain that – given the diverse nature of specific national contexts – the group will be able to achieve its objective of ensuring the consistent, EU-wide implementation of the provisions of the Second Payment Services Directive, compliance with the Delegated Regulation and a balanced approach for payment originators and account aggregators, which respects the interests of each party.

In November 2014, the UK Competition & Markets Authority launched investigations which led to the identification of breaches of competition in the provision of retail and small business banking services in the UK.[12] To open this market to new entrants, the CMA required the nine largest British banks to facilitate the exchange of banking data. An independent entity, the Open Banking Development Group, was tasked with specifying the APIs that the banks had to implement as from 13 January 2018[13] in order to communicate with the third party providers.

The French situation is quite different: it is the STET, a creation of the banks, which is responsible for developing the characteristics of the interfaces between French banks and third party providers.

The STET is taking a minimum approach of strict compliance and implementation of the interfaces by the 14 September 2019 deadline, i.e. twenty months after the major British banks. In this clearly defensive approach, neither account aggregators nor payment initiators, nor consumers are involved in the choice of specifications. Only the intervention of the National Cashless Payments Committee (CNPS), via the creation of an ad hoc working group, allows third party providers' needs to be taken into limited account.

[8] Prudential supervisors may, under strict conditions, exempt an account-keeping institution from the obligation to maintain a backup communication channel at all times (see recital 24 and Article 33(6) and (7) of Delegated Regulation 2018/389).
[9] Germany (Berlin Group), United Kingdom (Open Banking), France (STET), Poland (Polish Bank Association) and Slovakia (Slovakian Banking Association).
[10] See the minutes of the meetings on the European Payment Council website.
[11] The ECB ceased to be a member of the working group as from 3 September 2018.
[12] "Retail banking market investigation," Final report, Competition & Markets Authority, 9 August 2016.
[13] On 13 January 2018, the provisions of the Second Payment Services Directive were slated to enter into force simultaneously in all EU Member States.

The issue of savings and credit accounts

As its title suggests, the aim of the Payment Services Directive is better European integration of the retail payment market. The rules it stipulates and the rights it creates are valid only in the payment services field. However, the activity of account aggregators, like that of retail banking services, is broader. In addition to payment accounts, credit institutions' online banking sites generally provide access to accounts that support other services: credit reserves, savings accounts, securities accounts, insurance accounts, etc.

Of course, webscraping allows aggregators to collect all this information and return it to their customers, regardless of their legal status. The use of an aggregator-specific interface instead of webscraping, would result in a functional regression for aggregators if the interface did not provide information from every account.

The Second Directive prevents account aggregators from retaining their customers' bank connection identifiers by requiring them to refrain from requesting[14] "sensitive payment data linked to the payment accounts" (Article 67(2)), with sensitive payment data being defined as "data, including personalised security credentials which can be used to carry out fraud". However, the Delegated Regulation stipulates that banks that have set up a dedicated interface "shall ensure that this interface does not create obstacles to the provision of payment initiation and account information services" (Article 32(3)).

What will happen in September 2019 if the interfaces provided by some credit institutions restrict the information provided to account aggregators to payment accounts only? Will account aggregators continue to use webscraping for other accounts? Will the prudential authorities be able to exempt certain credit institutions from setting up a backup communication channel, while account aggregators would consider that the dedicated interface hinders their activity and does not fulfil its role?
The outcome of the dispute between banks and third party providers is uncertain. Account aggregators do not seem willing to retreat and surrender a portion of their business. It was not the intention of the Commission to restrict the activity of third party providers or the competition they impose on account-keeping institutions. The establishment of a dedicated communication channel is primarily motivated by security considerations and the efforts would be fruitless if account aggregators continued to hold their customers' bank identifiers.

Future challenges

In this case, the banks are being somewhat two-faced: it is interesting to note the gap between their collective expression, which is quite hostile to the very activity of account aggregators, and each institution's individual choices.

Boursorama, a subsidiary of Société Générale, rolled out an account aggregation service in 2008. Better still, since April 2017,[15] it has been possible to quickly and easily execute a transfer from an external bank account to an one held at Boursorama. Most banks now offer an account aggregation service on their online banking site. The purposes of account aggregation are generally twofold: a consumer services offer (BtoC), at the same time as a white-label offer for financial institutions that hold accounts (BtoBtoC).

[14] Payment originators appear to be entitled to request sensitive payment information, but they cannot store it (Article 66(3)).
[15] See Boursorama's press release of 3 April 2017: "Boursorama, première banque française à permettre à ses clients de réaliser des virements depuis des comptes bancaires externes."

Everyone has an agreed role in ongoing disputes and care should be taken not to lose sight of the general interest. The UK's "Open Banking" initiative has undeniably contributed to the creation of new innovative services. It has facilitated banking mobility, and has encouraged banks to offer more efficient and less expensive services. Although instant payment is expected to become a reality soon, the rise of third party providers is leading account-keeping institutions to provide real-time account management, which is much clearer for the consumer.

In a similar context, a few years ago, the airline company Ryanair claimed the right to distribute its airline tickets without intermediaries, through its website alone. However, without Ryanair's permission, the online travel agency Opodo developed a data capture system, which allowed it to offer seats on Ryanair flights for sale on its own website. With particular virulence, Ryanair brought Opodo to court, claiming contractual liability, violation of the rights of the database producer, trademark infringement, unfair competition and parasitism. The courts, however, dismissed every one of these claims.[16]

There is no doubt that third party providers will continue to offer new services and provide impetus to banks' offerings.[17] The combination of account aggregation and payment initiation services paves the way towards offers of daily offsetting accounts receivable with accounts payable, end-of-month investment when resources exceed expenses, etc. The analysis of banking transactions is likely to lead to useful recommendations for the consumer: when a loan or energy supply contract is too expensive compared to market offers, or when a reorientation of investments would be consistent with the asset objectives of the client concerned (robo-advisory).

The development of offers to enable households to make better financial decisions seems inevitable and likely to bolster consumers' attachment to their financial institution. On the strength of their European pre-eminence and brand image, the major French banks should not be associated with rearguard battles, but rather become involved in advice and innovation. The French public authorities should encourage them to do so.

[16] Ruling of 9 April 2010 of the Paris Court of First Instance, ruling of 23 March 2012 of the Paris Court of Appeal and ruling of 10 February 2015 of the Court of Cassation (Commercial division).

[17] The Second Payment Services Directive includes a review clause (Article 108) inviting the Commission to submit, by 13 January 2021 at the latest, a report on the application and impact of the Directive, accompanied, if necessary, by a legislative proposal.