With the support of the Erasmus+ Programme of the European Union

UNIVERSITÀ DI SIENA 1240

EUMOL Jean Monnet Chair in EU Money Law

EUMOL Lecture 10

Master Degree Students in International Accounting and Management (IAMA)

1. PAYMENT INITIATION SERVICE PROVIDERS AND ACCOUNT INFORMATION SERVICE PROVIDERS

When I explained the payment sevices I have already mentioned the payment initiation service and the account information services. In this case, the PSP hols the user's data rather than the user's funds. Indeed, preamble (28) PSD2 states that:

Moreover, technological developments have given rise to the emergence of a range of complementary services in recent years, such as account information services. Those services provide the payment service user with aggregated online information on one or more payment accounts held with one or more other payment service providers and accessed via online interfaces of the account servicing payment service provider. The payment service user is thus able to have an overall view of its financial situation immediately at any given moment. Those services should also be covered by this Directive in order to provide consumers with adequate protection for their payment and account data as well as legal certainty about the status of account information service providers.

When ever this kind of payment services are operated, it is established a separation between the PSP who holds the payment account and the account information service providers and the payment initiation service providers. The first one is defined in the PSD2 as a "payment service provider providing and maintaining a payment account for a payer".

PISP (this stands for Payment Initiation Service Provider) works as an alternative to paying online using a credit card or debit card. The new rules bring PIS within the scope of regulation, which will ensure that payment initiation service providers (hereinafter PISPs) receive access to payment accounts, whilst also placing requirements on them to ensure security for users.

PISPs must be authorized by the competent authority in their home Member State, setting out their business plan and operating model, demonstrating appropriate levels of initial and working capital, and specifying their risk management, financial controls,

fraud and security monitoring, and business continuity arrangements; in addition, they must hold a professional indemnity insurance or comparable guarantee to cover their liabilities in this respect.

AISP (this stands for Account Information Service Provider) provides the payment service user with consolidated information on payment accounts held by a payment service user with different payment service providers. PSD2 brings them within the scope of regulation, and this will ensure that account information service providers (hereinafter AISPs) can have access to payment accounts, whilst also placing requirements on them to ensure security for users. There is no minimum capital requirement for AISPs.

Both of them have accommodated in the experience of so-called 'open banking'. As Prof. Corvese wrote "This may be addressed as 'a movement "bridging two worlds", i.e. making possible for customers to use their banking and payment services in the context of other authorised third party (non-bank, Fintech) services, thereby combining innovative functionalities from banks and non-banks with reach through infrastructure".

PSD2 focuses on PISPs and AISPs: as long as they are properly registered, they can run professional payment initiation and account information services. In line with PSD2's pro-competitive goal, neither the provision of payment initiation services (Art. 66(5) PSD2) nor the provision of account information services (Art. 67(4) PSD2) 'shall be dependent on the existence of a contractual relationship' between PISPs or AISPs and the account-servicing PSPs. Indeed, in compliance with the right to data portability laid down in European Regulation no. 679 of 2016, the PSU enjoys the right to make use of payment initiation services (Art. 66(1) PSD2) and account information services (Art. 67(1) PSD2). In turn, the account-servicing PSP is in charge of creating the technical conditions to honour this right.

1.1. PAYMENT INITIATION SERVICES

The payment initiation service means a 'service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider' (Art. 4(15) PSD2). Therefore, this service establishes a dialectical relationship between the PISP and the account-servicing PSP. The latter is, generally speaking, a credit institution. In functional terms, this service can perform different tasks: it may 'create a software bridge between the customer and the online merchant (...) streamline and simplify the payment by the customer (...) [and] simplify the authentication'.

Concerning the first function, the payment initiation service may create a software bridge between the customer and the online merchant, giving him or her the assurance that the payment transaction can be initiated successfully. Considering the second function, 'the service can pre-set the amount and the beneficiary and eliminate the need to use the (separate) app or website of the bank'. In the end, a traditional authentication process that uses a card, a card reader or a personal identification number may be replaced by a mobile phone, a fingerprint, or facial recognition.

PSUs enjoy the 'right to make use' of a payment initiation service, as long as the payment account is accessible online, the right to be honoured by the account-servicing PSPs handling the payment transactions initiated through PISPs in the same way as orders directly transmitted by the payer. 'For this reason', it is argued, 'the bank is not allowed to charge a fee for the access to the account'. More specifically, whenever the payer gives his/her consent to initiate a payment transaction through a PISP, according to Art. 64 PSD2 the account servicing PSP has to fulfil the duties set out under Art. 66(4). This will:

(a) **'communicate securely with payment initiation service providers in accordance with point (d) of Article 98 (1)**'. Art. 35 of Commission Delegated Regulation on regulatory technical standards (hereafter, RTS Regulation) on the security of communication sessions establishes that accounting-servicing PSPs, PISPs, and the PSPs issuing cards and AISPs, 'ensure that, when exchanging data by means of Internet, secure encryption is applied between the communicating parties throughout the respective communication session in order to safeguard the confidentiality and the integrity of the data, using strong and widely recognised encryption techniques' (Art. 35(1) RTS Regulation);

(b) **'immediately after receipt of the payment order from a payment initiation service provider, provides or make available all information on the initiation of the payment transaction and all information accessible to the account servicing payment service provider regarding the execution of the payment transaction to the payment initiation service provider'**. Whenever online access to payment accounts is offered, account-servicing PSPs have to allow TTPs, like PISPs, to access the accounts under Art. 30(1) of the RTS Regulation. The Art. 31 RTS Regulation establishes that the account-servicing PSPs may either set up a separate dedicated interface or allow PISPs to use the users' interfaces. If they opt for the second type of access device, they cannot simply open the user interface since they cannot grant PISPs unlimited access to the accounts.

They are therefore bound to modify the interface to enable PISPs to 'identify themselves, to request and receive information on one or more designed accounts and associated transactions and to initiate a payment order'.

Criticism has been raised that account-servicing PSPs, mostly banks, may frustrate the PISPs' business. For example, they may set up dedicated interfaces by limiting the data available or reducing speed connections. To sidestep these technical obstacles, PISPs use 'screen scraping': this expedient allows them to gain access to payment accounts as if they were PSUs insofar as they receive the payers' personalised security credentials. However, when this happens, PISPs do not fulfil the duty of identification and gain access to more information than they are entitled to. This is why the EBA suggested prohibiting this option both in general and also as a 'fall back option'.

On the other hand, the European Commission has partially accommodated the requests from TTPs, and, in the final version of the RTS Regulation, a compromise was reached. Specifically, Art. 33 provides for contingency measures: once they have been identified, PISPs are entitled to make use of the interfaces made available to the PSUs and their authentication procedure if the dedicated interfaces do not perform properly.

Art. 33(1) RTS refers to cases of system breakdowns or unplanned unavailability. It is assumed that there is an event of this type after 'five consecutive requests for access to information for the provision of payment initiation services [or account information services] are not replied to within 30 seconds'.

(c) **'treat payment orders transmitted through the services of a payment initiation service provider without any discrimination other than for objective reasons, in particular in terms of timing, priority or charges vis-à-vis payment orders transmitted directly by the payer'**. PSD2 tries to prevent account-servicing PSPs from taking directly or indirectly anticompetitive measures against TTPs, which may in turn slow down the development of the payment services market. In addition, account-servicing PSPs must execute payment transactions according to the timeline laid down in the contract terms and conditions.

By contrast, Art. 68(5) PSD2 allows the account-servicing PSP to deny PISPs access to the payment account for 'objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access to the payment account by (...) that payment initiation service provider' while ever these reasons continue to exist. The account servicing PSP informs the payer that access is denied and why. This information should be given before the access is denied or immediately after 'unless providing such information would compromise objectively justified security reasons or is prohibited by other relevant Union or national law'. This is the case, for example, of money laundering controls. However, the business relationship between the PISP and the account-servicing PSP is not involved. In fact, whenever it denies access to a PISP, the account-servicing PSP has to immediately report the incident to the competent authority, giving details of the case and the reason for acting. In turn, the competent authority may take appropriate measures as a supervisory body.

Turning to the duties and obligations of PISPs, Art. 66(3) PSD2 sets out a series of conduct law rules for them. With regard to some aspects, these rules cover the contracting relationship with PSUs, but regarding some others they aim to protect the proper functioning of the payment system as a whole and thus potentially entail a supervisory relationship with the national competent authority. More specifically, PISPs must

(a) not hold at any time the payer's funds in connection with the provision of the payment initiation service;

(b) ensure that the personalised security credentials of the payment service user are not, with the exception of the user and the issuer of the personalised security credentials, accessible to other parties and that they are transmitted by the payment initiation service provider through safe and efficient channels;

(c) ensure that any other information about the payment service user, obtained when providing payment initiation services, is only provided to the payee and only with the payment service user's explicit consent;

(d) every time a payment is initiated, identify itself towards the account servicing payment service provider of the payer and communicate with the account servicing

payment service provider, the payer and the payee in a secure way, in accordance with point (d) of Article 98(1);

(e) not store sensitive payment data of the payment service user;

(f) not request from the payment service user any data other than those necessary to provide the payment initiation service.

(g) 'not use, access or store any data for purposes other than for the provision of the payment initiation service as explicitly requested by the payer';

(h) 'not modify the amount, the payee or any other feature of the transaction'.

Lastly, the matter of PISPs' liability and burden of proof for unauthorised payment transactions as well as for payment transactions that have not been correctly executed. The main aspect is the pivotal role performed by the account servicing PSP when the payment transaction is initiated through the PISP:

- Art. 73(2) obliges the account-servicing PSP to refund the PSU to the amount of the unauthorised payment transaction immediately or in any event not later than the end of the following business day. According to the same timeline, the account-serving PSP must, where applicable, 'restore the debited payment account to the state in which it would have been had the unauthorised payment transaction not taken place'. However, as long as the PISP is liable for the unauthorised payment transaction, it will immediately compensate the account servicing PSP 'at its request for the losses incurred or sums paid as a result of the refund to the payer, including the amount of the unauthorised payment transaction'. Lastly, Art. 73(3) establishes that, in a contracting relationship with a PSU, the PISP will make any further compensation established under national law;

- With regard to the burden of proof on the PISP, it is established that PISPs must prove that 'within its sphere of competence, the payment transaction was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency linked to the payment service of which it is in charge'. In other words, there is no normative difference between the liability standard set out for account-servicing PSPs and PISPs. This is also the case of the burden of proof rule according to Art. 72(2) PSD2:

2. Where a payment service user denies having authorised an executed payment transaction, the use of a payment instrument recorded by the payment service provider, ***including the payment initiation service provider as appropriate****, shall in itself not necessarily be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of the obligations under Article 69. The payment service provider, including, where appropriate,* ***the payment initiation service provider****, shall provide supporting evidence to prove fraud or gross negligence on part of the payment service user.*

1.2. ACCOUNT INFORMATION SERVICES

'Account information service' means 'an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider' (Art. 4(16) PSD2). Thanks to PSD2 this is a regulated activity: indeed, a business may enter the service market as long as it is specifically registered.

The access of AISPs is to be shaped in line with the PSU's access to payment account. With a view to honouring the PSU's right, Art. 67(3) establishes a series of duties and obligations for account-servicing PSPs. Indeed, account-servicing PSPs must

(a) communicate securely with the account information service providers in accordance with point (d) of Article 98(1);

and

(b) treat data requests transmitted through the services of an account information service provider without any discrimination for other than objective reasons.

At the same time, the PSD2 sets out a series of rules of conduct. Some of them cover the contracting relationship with PSUs, while others concern the supervisory relationship between the AISPs and the competent authorities. Indeed, they must:

> (a) provide services only where based on the payment service user's explicit consent;
>
> (b) ensure that the personalised security credentials of the payment service user are not, with the exception of the user and the issuer of the personalised security credentials, accessible to other parties and that when they are transmitted by the account information service provider, this is done through safe and efficient channels;
>
> (c) for each communication session, identify itself towards the account servicing payment service provider(s) of the payment service user and securely communicate with the account servicing payment service provider(s) and the payment service user, in accordance with point (d) of Article 98(1);
>
> (d) access only the information from designated payment accounts and associated payment transactions;
>
> (e) not request sensitive payment data linked to the payment accounts;
>
> (f) not use, access or store any data for purposes other than for performing the account information service explicitly requested by the payment service user, in accordance with data protection rules.

The proper application of these rules of conduct depends on the scope of account information services. The preamble (28) PSD2 provides that *Those services provide the payment service user with aggregated online information on one or more payment accounts held with one or more other payment service providers and accessed via online interfaces of the account servicing payment service provider. The payment service user is thus able to have an overall view of its financial situation immediately at any given moment.*

However, criticisms have been raised that the broad definition of account information service may weaken the directive limitations. For example, although Art. 67(2)(f) does not allow use of data to offer other products and services, the AISPs may sidestep this legislative limit by offering a broadly defined service. This is also true for providing data to a third party: the account information service becomes part of a 'more comprehensive relationship' such as a credit application. In this case, the AISP shares the data with a lender who wishes to use them for a personalised loan.

2. TRANSPARENCY RULES AND PAYMENT INITIATION SERVICES AND ACCOUNT INFORMATION SERVICES

Both the payment initiation service and the account information service have been newly laid down in PSD2 as payment services, so they may be carried out professionally as long as the business entity concerned has a a tailor-made licence. However, only the latter type of payment service seems to be strictly preparatory to a payment transaction execution and this might be the reason why only the PSD2 provides for tailor-made duties of information in this case. The PSD2 provisions concerned are articles 45 and 46, establishing a difference between information to be given before and after the payment transaction is initiated (or, in other words, the payment order is forwarded to the account servicing payment service provider).

In greater detail, before a payment transaction is initiated, the payer has to be informed aboutThe name of the payment initiation service provider, its head office, and its geographical address, as well as that of its agents or branches established in the Member States where the payment service is offered, together with further contact details of the PSP and the competent authority.

By contrast, 'immediately after' the initiation of the payment transaction, the payment initiation service provider will give confirmation to the payer (and, where applicable, the payee) of the successful initiation of the payment order with the payer's account servicing PSP and will give the payer

- a reference to enable them to identify the payment transaction
- the amount of the payment transactions
- the amount of charge payable, if any.

Concerning the way this information is provided in the PSP-user contractual relationship, PSD2 gives no clear-cut choice on the information to be provided or made available. In fact, articles 45 and 46 mention both of them. Despite the fact that the PSD2 provisions concerned are set out in Chapter 2 (Title III), covering the duties of information for single payment transactions, there is no sensible argument to exclude the possibility that the user has entered a framework contract with the payment initiation service provider. It explains the regulatory alternative (information provided and information made available) set out in the PSD2 articles concerned and leads to the conclusion that the way information is provided will follow the general distinction between transparency for single payment transactions and transparency for framework contracts.

References

Gimigliano, *Sub* Title IV, Arts 38-58 PSD2. Transparency of conditions and information requirements for payment services, in Bozina Beros, M. – Gimigliano, G. (eds), The Payment Service Directive II: a commentary, Elgar Commentaries Series, 2021 (in printing);

Gimigliano, *Sub* Title IV. Chapter 2 PSD2, in Bozina Beros, M. – Gimigliano, G. (eds), The Payment Service Directive II: a commentary, Elgar Commentaries Series, 2021 (in printing).