A NEW REGIME FOR ACCESS TO PAYMENT ACCOUNTS: THE PSD2

Carlos Conesa, Sergio Gorjón and Gregorio Rubio (*)

(*) Carlos Conesa and Sergio Gorjón are in the Associate Directorate General Financial Innovation and Market Infrastructures of the Banco de España. Gregorio Rubio is in the Directorate General Operations, Markets and Payment Systems of the Banco de España.

A NEW REGIME FOR ACCESS TO PAYMENT ACCOUNTS: THE PSD2

Abstract

The finance industry is currently facing a further competitive challenge, on top of ongoing digitalisation: a new type of payment service provider that acts either as an account information service provider or as a payment transaction initiator. These emerging entities, authorised under the Second Payment Services Directive of the European Parliament and of the Council, are now able to establish direct relationships with the customers of credit institutions, conducting transactions in their own name, without having to manage themselves a payment account, and accessing information of undoubted commercial value. This new scenario anticipates a change in the banking status quo and in banks' current business models, promising the development of new value propositions that will be to the benefit of bank customers and society as a whole. This article sets out the main changes introduced by the European Directive, highlights aspects still to be resolved and considers its possible impact on the different types of service providers.

1 Introduction

For some years now banks have been facing the challenge of how to improve their profitability in a setting marked by increasing regulatory demands and sustained low interest rates. This has been compounded recently by the potentially disruptive challenge of digitalisation, given the emergence and growth of new competitors from other industries.

While innovative initiatives are discernible in virtually every area of banking service provision, it is in retail payments that the emerging group of "FinTech firms" (see Chart 1) is having the greatest impact.

Given the importance of this business for financial institutions,[1] the industry has reacted by trying to speed up its digitalisation in an attempt to safeguard its leading role in payment services. Thus, for example, numerous steps have been taken, such as boosting mobile channels, promoting new ways of initiating transactions (contactless cards, QR codes, etc.) and reducing the time it takes for a payment order to be completed (e.g. instant payments). In parallel, traditional institutions, seeing opportunities to improve efficiency and to operate in other business areas that can provide alternative sources of revenue, are stepping up their collaboration with other players.[2]

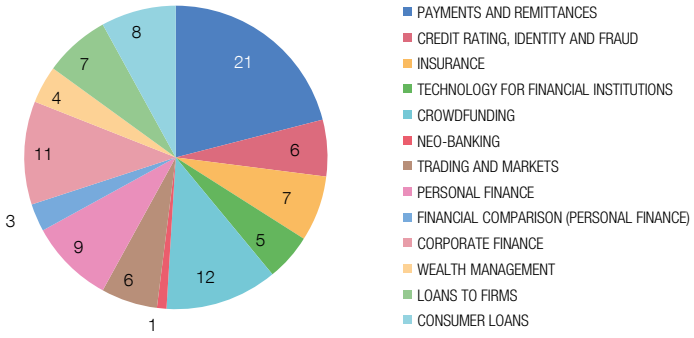
Against this background, the main legislation governing payment services in Europe has been comprehensively revised, providing players with new challenges and contributing to standardising the structure of the market. The Second Payment Services Directive *[Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market],*[3] known as "PSD2", is an ambitious and complex piece of legislation that aims to further accelerate the achievement of an integrated, competitive,

1 Fees and commissions have progressively played a bigger role in banks' income statements, given the contraction of net interest income; and, in particular, those associated with transaction and payment services. Thus, for instance, Ernst & Young estimate that the amounts received for charges on payment services provided by global financial institutions, without including net interest income, account for between 40% and 50% of their total revenue. In Spain alone, 2016 fees and commissions, which include other activities such as those relating to investment funds, employee pension and insurance schemes and operations with securities, gave rise to revenue of €8,839 million for the eight listed credit institutions. This figure was 1.2% up on the previous year and accounts for 32.6% of their recurring billings (net interest income plus fees and commissions).

2 These sources are largely, though not exclusively, based on the harnessing of personal data to personalise services, marketing and advertising.

3 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN.

FINTECH FIRMS BY FINANCIAL SERVICES CATEGORY (%) CHART 1



SOURCE: Finnovista.

innovative and efficient market for payment services in the EU, without undermining user safeguards. Hence the importance the Directive attaches to aspects relating to the security of payment services and, in particular, to regulating the activities of new entrants that bank customers may authorise to access their payment accounts at a different financial institution.

This article sets out the main changes introduced by the European Directive and its implementing legislation, highlighting certain aspects still to be resolved and addressing the possible impact on different types of service providers. Following this introduction, Section 2 analyses the PSD2 in detail, focusing first on security-related aspects and then describing the new account information and payment initiation services, analysing the various communication channels between account servicers and entities that provide these new services and, finally, detailing the interaction between the various types of providers and the main problems still to be resolved. Section 3 includes some of the possible effects of the PSD2 and considers its potential impact on the various types of providers. The article ends with a section devoted to drawing the main conclusions.

2 The PSD2: the regulatory framework as a galvanising factor

In Europe, the regulator has not wished to remain a mere spectator to the far-reaching changes taking place in payment services. A fundamental part of such changes has been the result of plans for a broad range of measures that meet users' new expectations and ultimately aim to achieve a more robust and integrated European economy. Initiatives include most notably the European Commission's proposal for *A Digital Single Market Strategy for Europe* (2015)[4] and, more recently, the *Consumer financial services action plan: better products, more choice.*[5]

However, in the payments area the main focus has been on the revision of the first Payment Services Directive (Directive 2007/64), known as "PSD1", the basic legislation regulating these services for many years, which was superseded by PSD2 in 2015. The new Directive includes two major changes: a) greater attention to the risks associated with the new

4 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=ES.

5 http://eur-lex.europa.eu/resource.html?uri=cellar:055353bd-0fba-11e7-8a35-01aa75ed71a1.0013.02/DOC_1&format=PDF and its annex http://eur-lex.europa.eu/resource.html?uri=cellar:055353bd-0fba-11e7-8a35-01aa75ed71a1.0013.02/DOC_2&format=PDF.

strategies arising from the digital transformation and, b) an extension of its scope to cover new payment services.[6]

2.1 THE PSD2 AND SECURITY MEASURES FOR ELECTRONIC PAYMENT TRANSACTIONS

As regards payment transaction security, the PSD2 focuses particularly on remote payment transactions, whether via Internet or using mobile devices. This emphasis is a direct consequence of the notable increase in these transactions in recent years, boosted by the e-commerce boom (see Table 1).

Building on the recommendations of the ECB *(Recommendations for the security of internet payments)*[7] and the European Banking Authority's (EBA) guidelines *(Guidelines on the security of internet payments),*[8] the PSD2 has made the security of electronic payments one of its main pillars. The Directive requires specific security measures and procedures to be applied in electronic payment transactions and, in particular, in those carried out remotely.

These measures and procedures are based on the concept of "strong customer authentication",[9] the main characteristics of which are summarised in Table 2.

It was not possible, however, to give a detailed definition of strong customer authentication in the Directive, owing to the technical complexity of this concept and the granularity that would have had to be included, but also because of the great diversity of the cases subject to its application. Consequently, the PSD2 confined itself to laying down a series of general principles, and entrusted development of the detailed legal framework that should govern the security of electronic payments to the EBA, in collaboration with the ECB.

To this end, the EBA began work on drafting *Regulatory Technical Standards (RTS) on strong customer authentication and common and secure communication.*

These RTS include the main features of strong authentication, seeking to be neutral from a technological standpoint and respecting the different business models. They also include certain exceptions, depending on the risk of the transaction, its amount and the channel through which it is conducted (see Table 2). The RTS likewise set out the legal arrangements applicable to access to payment accounts, a vital aspect when determining how the different payment service providers will interact. This is explained in greater detail in the following section.

After a tortuous process, the RTS eventually led to *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,*[10] published on 13 March 2018.

---

6 Along with this, the PSD2 introduces other fine-tuning measures relating, in the main, to its scope of application and to the prudential arrangements for the payment service providers it specifically regulates (payment institutions).

7 http://www.ecb.europa.eu/pub/pdf/other/pubconsultationoutcome201405securitypaymentaccountaccessservicesen.pdf?3b8c24c7dc9fa5f57204d212c66f2dc7.

8 https://www.eba.europa.eu/documents/10180/1004450/EBA_2015_ES+Guidelines+on+Internet+Payments.pdf/44d07cf8-1721-4407-94a6-3a8c256149fa.

9 SCA, by its abbreviation.

10 – https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2018.069.01.0023.01.SPA&toc=OJ:L:2018:069:TOC.

B2C E-COMMERCE TURNOVER FIGURES (2011-2016) (a) TABLE 1

$bn

	2011	2012	2013	2014	2015	2016
North America	327.77	373.03	419.53	469.49	523.09	580.24
Asia-Pacific	237.86	315.91	388.75	501.68	606.54	707.60
Western Europe	218.27	255.59	291.47	326.13	358.31	387.94
Eastern and Central Europe	30.89	40.17	48.56	57.96	64.35	68.88
Latin America	28.33	37.66	45.98	55.95	63.03	69.60
Middle East and Africa	14.41	20.61	27.00	33.75	39.56	45.49
WORLD TOTAL	**856.97**	**1,042.98**	**1,221.29**	**1,444.97**	**1,654.88**	**1,859.75**

SOURCE: eMarketer (2013).

a These include purchases via any digital channel (PC, mobile and tablets) of travel, digital downloads and tickets for events. On-line gambling is excluded. The totals may not coincide with the sum of the individual items due to rounding.

However, this article retains references to the RTS for two reasons. First, in view of market practice, which prefers to continue referring to this Delegated Regulation as *RTS on Strong Customer Authentication and Common and Secure Communication.* And further, because this Regulation will only apply from 14 September 2019. In any event, references to the RTS should be understood as being to Delegated Regulation (EU) 2018/389.

2.2 NEW PAYMENT SERVICES UNDER THE PSD2: PAYMENT INITIATION SERVICES (PISS) AND ACCOUNT INFORMATION SERVICES (AISS)

Traditionally, credit institutions have been the main providers of payment services, to their current-account holding customers. The PSD1 regulated payment services in detail and laid down the vetted access principle, which restricted such services to authorised entities subject to supervision, which became generally known as payment service providers (PSPs).

Basically, this term included credit institutions and payment institutions.[11] The main innovation of the PSD1 was, precisely, the creation of this latter type of service provider, with a supervisory regime proportionate to the risks of their activity, which was restricted to payment intermediation, in contrast to the broad range of services characterising the operations of credit institutions.

However, the services provided by some specialist institutions to the holders of accounts at other institutions remained outside the scope of the PSD1 and, therefore, these were

– Prior to this, the EBA had published its proposal on 23.02.2017: https://www.eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+%28EBA-RTS-2017-02%29.pdf.
– In a letter addressed to the EBA, the European Commission announced on 24.05.2017 its intention to make certain changes to specific articles of the RTS proposed by the EBA. These changes can be viewed in: http://www.eba.europa.eu/documents/10180/1806975/%28EBA-2017-E-1315%29%20Letter+from+O+Guersent%2C%20FISMA+re+Commission+intention+to+amend+the+draft+RTS+on+SCA+and+CSC+-Ares%282017%292639906.pdf/efbf06e1-b0e9-4481-88e5-b70daa663cb9.
– This letter led the EBA to issue an Opinion on 29.06.2017 in which it expressed its position on the changes announced by the European Commission: https://www.eba.europa.eu/documents/10180/1894900/EBA+Opinion+on+the+amended+text+of+the+RTS+on+SCA+and+CSC+%28EBA-Op-2017-09%29.pdf/df60c6ac-a284-4772-b1d5-66c7073d28af.

11 Electronic money institutions, along with post office giro institutions and the public and monetary authorities in certain circumstances, are also part of the group of payment service providers. Nonetheless, given that the market share of these institutions and agencies is very small, and since the regulation of electronic money institutions in their capacity as payment service providers is the same as that for payment institutions, in this article, for the sake of simplicity, the term payment institutions refers to all these payment service providers and, in particular, to electronic money institutions when they act as such providers.

MAIN REGULATORY CHARACTERISTICS OF STRONG CUSTOMER AUTHENTICATION UNDER THE PSD2 TABLE 2

Strong Customer Authentication under the PSD2

Involves: authentication based on the use of two or more independent security elements		Security features:	— Knowledge (something only the user knows) — Possession (something only the user possesses) — Inherence (something the user is)
		Independent:	— The breach of one does not compromise the reliability of the others — No requirement for different devices
		Personalised security credentials:	Personalised security features provided by the payment service provider (PSP) or linked by the PSP to the customer
Obligatory if:	— Online payment account access — Electronic payment transaction — Remote action entailing risk — Presence of a TPP	Dynamic security feature if:	— Remote electronic payment transaction — Presence of a PISP
Possibility of exemptions based on:	— Level of risk (TRA) — Amount — Channel		
Accompanied by:	Transaction monitoring mechanisms		

SOURCE: Banco de España.

provided within the EU without being specifically regulated. The main services of this type are the initiation of a payment in an account of another institution (known as a payment initiation service or PIS) and the offering of consolidated information on the outstanding balances and transactions on more than one payment account at different institutions (known an account information service or AIS). The fundamental characteristic of these services is that the provider does not need to service a payment account; rather, it needs the customer's consent to operate or obtain information on accounts held at other institutions. Firms that have specialised in these types of services are "third-party firms" in the traditional bilateral relationship between the PSP and its customer; accordingly, they are usually called third-party providers (TPPs).

Initially, and until the RTS implementing the PSD2 come into force, the main method used by TPPs to gain access to their customers' payment accounts at other institutions involved using customers' personalised security credentials. Hence, TPPs would request the credentials of account holders and access their customers' accounts in the same way and with the same credentials as the holders themselves,[12] using techniques habitually referred to as "screen scraping". From a technical standpoint, screen scraping is a programming method which, through reverse engineering, enables data to be extracted from a screen-displayed representation (via a website or a pdf file, for example) and uploaded onto another application. In banking, this technique enables any entity with access to a customer's online payment account to extract and use the account data.

Operating in this way had security and efficiency implications since, without identifying themselves, TPPs (not linked to the account servicing entity) could gain access to customer

12 There has been and continues to be much debate on whether this practice complies with Directive 2007/64/EC or PSD1, as the sharing of personalised security credentials may be understood as a breach of the obligations imposed by the Directive upon the payment service user. However, as the Directive does not expressly forbid such sharing, its prohibition in the context of new payment services has been dismissed by some courts on the grounds that it would restrict free competition.

data using a channel intended for the customer itself. Therefore, TPPs were "impersonating customers" and could potentially access more information than was strictly necessary to provide the services requested by such customers. This situation was possible because, as a general rule, account servicing entities set up a single mechanism for access to all the accounts, products and positions of their customers.[13] Through this route, TPPs were therefore able to obtain full view of the customer's overall position, without the customer necessarily being aware of this and regardless of the scope of the permission granted.

However, payment initiation or account information services may offer useful solutions to merchants and consumers (such as a consolidated view of their balances and transactions) or alternative payment channels for online commercial transactions that do not require the use of specific payment instruments, such as payment cards. Also, as part of the widespread shift towards "open banking",[14] it may be thought that PSP customers should be able to use their own information and assign it to third parties if they so wish. Consequently, the PSD2 is a response to the regulator's aim of allowing these payment initiation and account information services (PISs and AISs) to be developed and consolidated, in a setting that provides consumers with adequate protection both for their payments and for the information associated with their accounts.

Additionally, the PSD2 entitles any holder of a payment account that is accessible online to initiate a payment order through a PSP other than the one at which the account is open. The Directive also recognises the right of any holder of one or more payment accounts accessible online to gain access to the information contained in the accounts through a payment service provider other than that or those at which the account(s) is/are open. In other words, AISs and PISs are included within the regulatory perimeter, with the appropriate safeguards, to provide consumers with adequate protection.

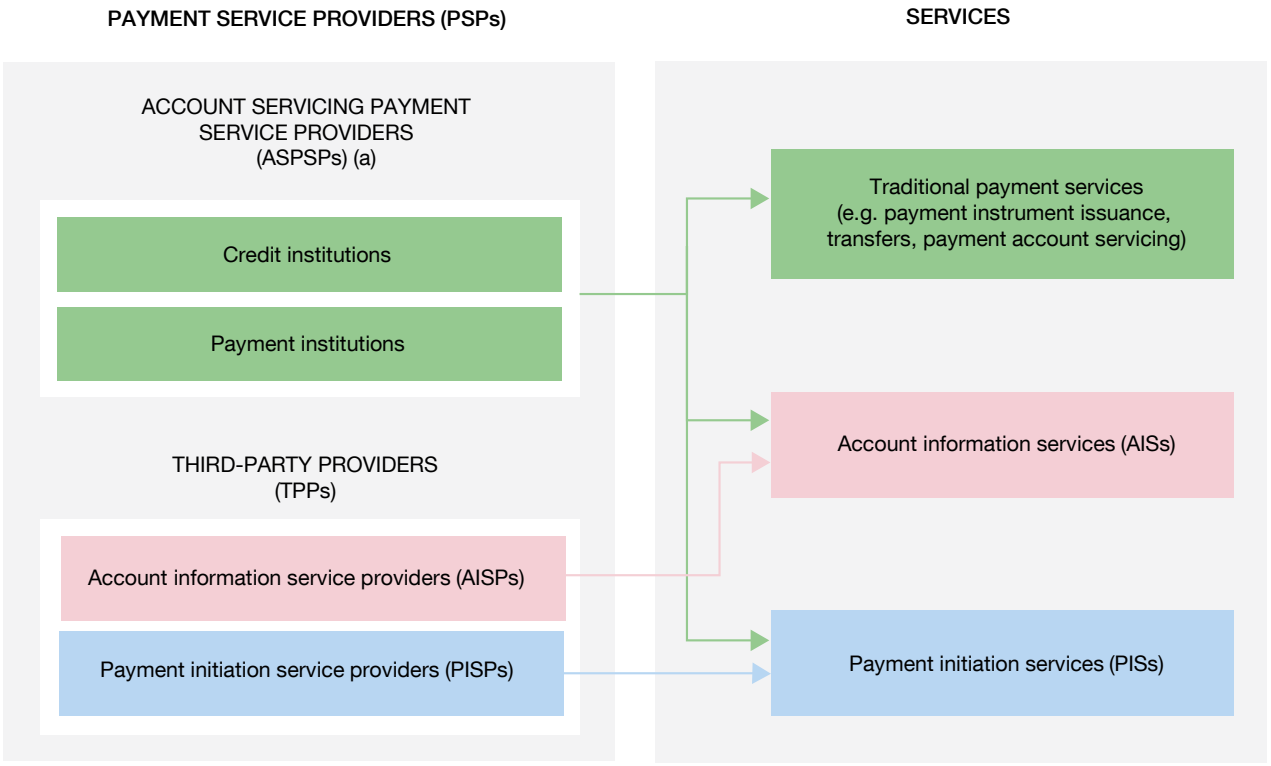
The PSD2 allows for the existence of PSPs that only provide PISs or AISs, without directly servicing payment accounts. Accordingly, the set of entities that are recognised as PSPs has been expanded, resulting in a complex landscape (see Scheme 1). PSPs are divided into two basic groups: those which service their customers' payment accounts, commonly known as "account servicing payment service providers" (ASPSPs), and TPPs which provide AISs or PISs, without servicing customer accounts.[15] The first group basically includes credit institutions and payment institutions, while in the second group, a distinction is usually drawn between payment initiation service providers (PISPs) and account information service providers (AISP). It is important to note, however, that ASPSPs may provide all manner of payment services, including PISs and AISs, and that TPPs may provide both payment initiation services and account information services, provided they comply with the applicable regulatory requirements (see Table 3).

13 This is the way things are done for reasons such as maximising customers' user experience, commercial policy, reducing costs, ease of maintenance, application updating, etc.

14 Open banking can be defined [Brodsky and Oakes (2017)] as a collaborative model in which banking data are shared between two or more unrelated actors to provide services to the market. Although it is not strictly necessary, it is usually assumed that data exchanges between banks take place through application programming interfaces (APIs). APIs are standard communication interfaces that enable information to be exchanged between computer applications. This is dealt with in greater detail in the next section.

15 Some payment services, such as money remittance, for example, do not require the existence of payment accounts.

PAYMENT INSTITUTIONS AND SERVICES SCHEME 1



SOURCES: European Payments Council and Banco de España.

a For the sake of simplicity, only the main categories of ASPSP are included (credit institutions and payment institutions). There are, however, other less significant institutions which may act as ASPSPs, such as, for instance, electronic money institutions and post office giro institutions.

The PSD2 sets out the prudential requirements for entities acting solely as PIS or AIS providers.[16] Owing to the limited activities carried out by these entities (and the risks inherent in them), these requirements are less stringent than those applicable to entities that service payment accounts. Table 3 provides a summary of the main requirements applicable to the various different categories of PSPs.[17]

The PSD2 also establishes the basic rules necessary to regulate the exchange of information between ASPSPs and entities providing AISs and PISs, which are summarised in Table 4. A fundamental aspect determining the interaction between these two groups of providers is the possible absence of a contractual relationship between them, since under the PSD2 a specific agreement between the account-servicing provider and the entity providing payment initiation or account information services is not required. Also, the latter entity will be entitled to use the authentication procedures that ASPSPs have provided to their own customers. In addition, the Directive does not allow unjustified discrimination against orders given by a user through a PISP or an AISP, in particular in terms of timing, priority and charges.

16 These requirements refer to payment service providers that are not subject to other prudential requirements owing to their nature, i.e. those applicable to payment institutions acting as ASPSPs.

17 In the case of ASPSPs, payment institutions are considered, since credit institutions are subject to stricter requirements owing to the wide range of services they provide.

PRUDENTIAL REQUIREMENTS UNDER THE PSD2 TABLE 3

Comparison between the requirements applicable to payment service providers that only provide payment initiation or account information services and those applicable to account-servicing payment service providers.

Criterion	ASPSP	PISP	AISP
Payment services	All	Payment initiation	Information on payment accounts and designated payment transactions
Possession of customer funds	Yes	No	No
Minimum capital (€)	125,000	50,000	No
Own funds	Yes	No	No
Professional indemnity insurance	No	Yes	Yes
Authorisation	Yes	Yes	No
Registration	Yes	Yes	Yes
Passport	Yes	Yes	Yes
Organisational requirements	All	All	Security and continuity-related only
Application of the PSD2	Yes	Yes	Limited: supervision plus information and security requirements
Possibility of exemptions	Yes, based on average value of payment transactions, with loss of passport	No	Yes, mandatory and without loss of passport

SOURCE: Banco de España.

As a result of the foregoing, ASPSPs are required to facilitate customer operations through PISPs and AISPs (which in practice act like direct competitors of ASPSPs), even if they are unable to receive any specific consideration for doing so.[18] This approach has very broad implications since, in the absence of a contractual relationship between an ASPSP and an AISP or PISP, the way in which these two groups of entities, often with conflicting interests, should exchange information sensitive for their common customer in a secure manner must be laid down in the PSD2 and its implementing regulations (RTS). The following sections analyse in greater detail how the PSD2 tackles this particular issue.

2.3 INTERACTION BETWEEN PAYMENT SERVICE PROVIDERS UNDER THE PSD2: DIRECT ACCESS VERSUS DEDICATED INTERFACE (API)

The situation described in the preceding paragraphs evidences the increasing importance of security-related aspects in the regulation in connection with access to payment accounts. For this reason, the PSD2 imposes the use of common and secure open standards of communication (CSC) for identifying entities, authenticating customers and notifying information, and for implementing the security measures that should govern relationships between the different payment service providers participating in a transaction. Thus, the aim is to ensure the integrity of funds, the confidentiality of information and the safeguarding of users' personalised security credentials.

However, the Directive does not prescribe a specific communication standard. Instead, it mandates the EBA to specify, in close collaboration with the ECB, the requirements to be met by such standards so that they are in line with the spirit of the Directive. The PSD2 only states that such standards must at least ensure the interoperability of different technological

18 ASPSPs must apply to TPPs the same conditions they would apply to their customers if the latter were carrying out the transaction directly rather than through an intermediate entity. Therefore, ASPSPs cannot charge TPPs additional fees and are obliged to provide services free of charge if the direct consultation of information or initiation of payment is free of charge for the customer, as is usually the case.

OPERATIONAL FRAMEWORK APPLICABLE TO PISPS AND AISPS

TABLE 4

Criterion	PISP	AISP
Service linked to existence of online accounts	Yes	Yes
Contractual relationship with ASPSP	No	No
Obligation to identify itself to ASPSP	Yes	Yes
Possibility of using credentials and authentication procedures provided by ASPSP	Yes	Yes
Obligation to use SCA	Yes	Yes
With dynamic element	Yes	No
Obligation to use CSC	Yes	Yes
Information and security credentials safeguard	Yes	Yes
Existence of a framework agreement with the payer	No	Yes
Possibility of access being refused by ASPSP	Only if there are objective and documented grounds	Only if there are objective and documented grounds
Discrimination between orders by ASPSP	No	No

SOURCE: Banco de España.

communication solutions and permit the use of all kinds of devices commonly used in the market in connection with payment services.

Conversely, the PSD2 does expressly address one of the most controversial aspects of the main method used to date to access payment accounts by a third party: TPPs "impersonate customers" using their personalised security credentials and gaining access to their accounts in the same manner and with the same permits as the account holders, without identifying themselves as a third party. To mitigate the risks associated with this practice, the PSD2 obliges PISPs and AISPs to identify themselves to the ASPSP every time they access a customer's payment accounts. However, it does not prescribe a specific access model. Under the RTS, such identification is to be through the use of qualified certificates for electronic seals or for website authentication,[19] which ensure the origin and authenticity of the data associated with a legal entity and authenticate the website linked to it, respectively.

However, the Directive does not expressly address the practice of "screen scraping", which therefore falls solely within the scope of the RTS on communication standards.

In light of this, the RTS do not impose a specific form of access, allowing both that known as "direct access" and the setting up of "dedicated interfaces".

– *Direct access* consists in the use by a TPP of the communication channel established by the ASPSP for its customers (usually an online banking application), which is the customary channel on which PISPs and AISPs have based their business models and which they have been using to date to access information on their customers' payment accounts using "screen scraping" techniques. A priori, this is the access most commonly preferred by TPPs,

19 The two certificates are defined by Articles 3(30) and (39), respectively, of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG).

COMPARISON BETWEEN THE REGIME FOR ACCESS TO PAYMENT ACCOUNTS UNDER THE PSD2 AND THE UK OPEN BANKING INITIATIVE

TABLE 5

PSD2	UK Open Banking
It is mainly a **regulatory framework.**	It is mainly a **business philosophy.**
It is the tool chosen by the **European authorities** to integrate retail payments in the EU.	It is the path chosen by **UK authorities** to put an end to the retail banking status quo in the United Kingdom.
Its **main purpose** is to harmonise payment services in the EU, provide security in the payment chain and protect consumers.	Its **main purpose** is to increase competition in the banking industry, enhance efficiency and foster innovation.
To this end, it establishes the **security measures** for the provision of payment services, includes all **payment services** in the regulated perimeter and sets the prudential and operational requirements that must be met by **payment service providers.**	To this end, **access** by authorised third parties was first opened (March 2017) to certain **standardised information,** such as banking products and reference data and, subsequently (January 2018), to personal and SME **current accounts.**
This should lead to greater competition in equivalent conditions across the EU and, therefore, to innovative, efficient, convenient and secure **payment services and methods.**	The former enables the map of **retail banking products and services** (including payment products and services) in the United Kingdom to be traced; the latter enables: i) such products and services to be **personalised,** either by their first providers or by duly regulated third entities, and ii) initiation and information services to be rendered.
Based on a holistic approach to payment services, it regulates **access to payment accounts by authorised third parties,** whether to initiate payments or to obtain aggregated account information.	**Access** to current accounts by third parties is carried out through application programming interfaces **(APIs),** based on an **open standard** which governs the **secure** sharing of data.
It does not establish any specific form of **access** to payment accounts, but does set the **conditions** under which such access should take place; it is account payment service providers which determine access by third parties to payment accounts.	The **standard** was developed by the Open Banking Implementation Entity, which was founded in 2016. Its governance, composition and funding was determined by the UK authorities; the **nine** largest **banks and mortgage companies** in the United Kingdom participate in it and they are required to apply the standard.
The access conditions are set out in the RTS laid down by the EBA in collaboration with the European Commission. **All account servicing payment service providers** should provide a means to access payment accounts that meets these conditions, but no standard is specified. However, European authorities have shown their preference for the use of APIs for such access and they trust the industry as whole will design the **standards** accordingly.	The **design** follows the recommendations of the Open Banking Working Group and the applicable mandates of the PSD2.

SOURCE: Banco de España.

which were already providing these services before the implementation of the PSD2. A substantial change wrought by the PSD2 in the use of this channel is that TPPs are now obliged to identify themselves as such when gaining access to customer information.

– Access by means of a *dedicated interface* involves the development by the ASPSP of a specific communication channel for the TPP other than the online one used by the entity's customers. Although not specified by the RTS, the practical implementation of this option will generally be assumed to take place through application programming interfaces (APIs), the technique currently used by the industry for interconnection and development of applications.[20]

This lack of specification is precisely one of the most significant differences between the opening of payment accounts promoted by the PSD2 and the general concept of "open

20 APIs are a technique that enables two software applications to be connected to each other to access their functionalities by exchanging messages or data in standard format.

banking", which is strictly linked to the opening of accounts through data structuring and the use of standardised APIs. One of the most salient examples of open banking is the UK's open banking initiative. Table 5 briefly summarises the main differences and similarities between this initiative and the PSD2. Although the differences are mainly the result of the different objectives underlying the two operational frameworks, the similarities are such that they allow the PSD2 to be included in the broad concept of open banking.

In any event, and whichever the option finally chosen by an ASPSP to transfer data, it should allow for secure communication between the ASPSP and the TPP and, as noted previously, for the identification of third parties to the ASPSP. It should also permit the use of any authentication procedures implemented by the ASPSP. Additionally, since the access mechanism should be based on open, common and secure communication standards, the interfaces should follow communication standards issued by European or international standardisation organisations and their technical specifications should be documented and made available free of charge to the AISPs and PISPs at least six months[21] prior to the implementation date. The PISPs and AISPs will have in place sufficient mechanisms to validate their applications and programmes over an equivalent period of time.

2.4 THE DISCUSSIONS ON RTS AND CHALLENGES PENDING

The EBA has faced numerous difficulties setting the legal regime for access to payment accounts by PISPs and AISPs; reconciling the multiple and, on occasions, contradictory objectives pursued by the PSD2 has proven complicated.

From a technical viewpoint, the decision had to be made whether to draft highly detailed RTS, unequivocally strengthening the security of the standards (with the danger of linking RTS to a specific technology) or whether to formulate a number of broad, durable principles that would not prejudice innovation (at the risk of not sufficiently strengthening security). From the perspective of homogenisation, the choice was between precise regulation, ensuring an adequate degree of harmonisation at European level, and the introduction of more flexible standards, permitting the development of different payment solutions within the EU.

The main problems, however, have arisen due to the different approaches of the various types of suppliers and their conflicting interests. Given the direct competition between the agents involved, it was sought when drafting the RTS to find the best way of reconciling the legitimate interests of the PISPs and AISPs, on one hand, and of the ASPSPs, on the other. Moreover, regulations do not allow the relations between them to be adjusted contractually in order to establish appropriate security measures for the risks introduced or to agree appropriate consideration for access to a very costly infrastructure. This latter circumstance meant, moreover, that the PISPs and the AISPs were openly distrustful of any mechanism to access payment accounts other than the direct access the ASPSPs provide to their customers, since they considered that there were no incentives for ASPSPs to offer truly effective and operationally reliable solutions through purpose-designed APIs.

To dispel the above-mentioned distrust, the RTS explicitly provided that the dedicated interfaces would have to offer, at all times, availability and performance levels at least as high as those of the direct accesses (online banking interfaces), while introducing an

21 In the EBA's initial proposal this period was three months, which in the final resolution of the European Commission is maintained only for subsequent interface modifications.

obligation to monitor such levels and to make the resulting statistics available to the national competent authority. Also, dedicated interfaces were required to have contingency mechanisms equivalent to those of direct accesses, in case dedicated interfaces did not operate with the same levels of availability and performance as online banking interfaces.

However, PISPs and AISPs declared in various fora that these contingency measures might be insufficient. In their opinion, these proposals did no more than establish mechanisms to restore, without delay, the availability of the dedicated interface, without guaranteeing its proper functioning at all times and, as a result, could jeopardise the continuity of the activity of PISPs and AISPs. This view was shared by the European regulator, which, as a result, opted to include in the RTS measures to encourage ASPSPs to implement truly efficient dedicated interfaces.

Consequently, the European Commission promoted inclusion among the contingency measures[22] of the so-called fall-back mechanism, which enables PSPs and AISPs to make use of direct access via the interfaces that ASPSPs offer their customers directly through online banking, in the event that the dedicated interface does not function correctly. The problem with this proposal is that its mere existence is a powerful disincentive to dedicated interfaces being developed, as it means that ASPSPs will not only have to implement the specific relevant interfaces but will also have to adjust their online banking interfaces to the provisions of the RTS should they have to be used by PISPs or AISPs under the fall-back mechanism.

To avoid these collateral effects, the European Commission has contemplated the possibility that national competent authorities may, after consulting the EBA, exempt ASPSPs from the obligation to adapt their online banking interfaces (direct access) to the rules laid down in the RTS, provided that they fulfil certain requirements. Notable among these are that dedicated interfaces must be designed and tested to the satisfaction of PISPs and AISPs, and used for at least three months to verify that any incidents are resolved without undue delay.

The European Commission's solution seeks to balance the interests and obligations of the two parties, but its practical implementation poses some significant challenges. On one hand, the RTS lack a desirable level of detail on questions such as key performance indicators, objective service levels and the requirements that dedicated interfaces must satisfy to be exempt from the implementation of the fall-back mechanism. This lack of precision is exacerbated by the fact that the evaluation of performance and service level compliance is performed by the parties in conflict (ASPSP, PISP and AISP), to whose satisfaction it must be possible to validate the dedicated interfaces.

The EBA is working on guidelines on the conditions to be met to enable the exemption from the obligation to adapt online banking interfaces to the rules laid down in the RTS to be granted. The aim is to mitigate the lack of detail mentioned above and, at the same time, to facilitate the necessary prior consultation by the national competent authorities so

22 According to the RTS, the contingency measures must be activated when the functioning of the specific interfaces is not in line with the RTS requirements or when such interfaces are not capable of attending to five consecutive access petitions within 30 seconds. For the purposes of evaluating the functioning of the specific interfaces, ASPSPs must define fully transparent key performance indicators, as well as objective service levels, that must be at least as stringent as those for online banking interfaces. The interfaces, indicators and objectives must be monitored by the authorities and submitted to stress tests conducted by ASPSPs.

that ASPSPs may be exempted from implementing the fall-back mechanism. To this end, on 13 June 2018 the EBA published the relevant consultation document, inviting all interested parties to submit any comments they might deem appropriate.[23]

However, these guidelines will not be sufficient to mitigate a second factor of uncertainty arising from the lack of specification of common and secure open standards of communication satisfying the requirements laid down in the RTS. This means that ASPSPs do not have valid references when designing the dedicated interfaces, which may hamper the rollout of effective solutions consistent with the RTS in a time and resource-limited environment.

As if that were not enough, the lack of detail in the RTS on the access of PISPs and AISPs to payment accounts via online banking interfaces (direct access) is another significant obstacle to implementation of the RTS. In this respect, the RTS merely recall that these suppliers must take all measures necessary to comply with the operating restrictions imposed by the PSD2 and, in particular, the ban on accessing, storing or processing customer data for a purpose other than the service contracted. No specific measures are offered to ensure compliance beyond some provisions relating to transaction recording and notification. One foreseeable consequence will be that, insofar as screen scraping continues to be a habitual access method, compliance with the requirements of the PSD2 by PISPs and AISPs will depend on self-imposed restraint by the latter.

Mindful of these problems, the European Commission has promoted the creation of an analysis group with representatives from all the relevant parties. The aim is to establish the basic functionalities that must be met by APIs for which validation of adaptation to the RTS is sought. For this purpose, among other initiatives, the group intends to informally review the technical specifications of some standardised pan-European APIs. This will provide a reasonable number of standards in line with the requirements of the RTS and PSD2 that can serve as a reference for the ASPSPs and for the respective national authorities.

The European Commission trusts that this analysis group will be able to complete the RTS effectively and consensually, fostering the widespread implementation of dedicated interfaces based on a limited number of standardised APIs. This would ensure the eradication of screen scraping and, moreover, lay the foundations for extensive use of a business model truly based on an open banking environment, albeit limited to payment accounts. In addition, this would help ensure compliance with other regulatory provisions, in particular those relating to data protection.

However, the experience of the work carried out here by the Euro Retail Payments Board[24] highlights the difficulties involved in reaching agreement in areas as important as the

---

23 This consultation document is available at: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-the-conditions-to-be-met-to-benefit-from-an-exemption-from--under-article-33-6-of-regulation-eu-2018/389-rts-on-sca-csc-.

24 The Euro Retail Payments Board (ERPB) was created in December 2013 by the ECB to replace the SEPA Council, with the aim of promoting an integrated, innovative and competitive market for retail payments in euro in the European Union. At the end of 2016, the ERPB decided to set up a working group on payment initiation services which presented its final report in November 2017. This report is available at: https://www.ecb.europa.eu/paym/retpaym/shared/pdf/8th-ERPB-meeting/PIS_working_group_report.pdf?483e4d28242cd84322850a01e549d116.
As regards the technical aspects of APIs, the work of this group is being continued by the analysis group promoted by the European Commission,
A second report by this group, relating to other requirements necessary for European integration of payment initiation services, may be consulted here: https://www.ecb.europa.eu/paym/retpaym/euro/html/index.en.html.

treatment of the consent of the payment account holder, the sphere in which customer authentication should occur, the information that the ASPSP must provide to the PISP, the combined provision of payment initiation and account information services or key indicator identification.

In order to ensure smooth implementation of the RTS, the analysis group promoted by the European Commission must not only be capable of completing this work but also of aligning its interpretations with those of the national authorities and of the EBA in the area of their respective competencies. For there to be a chance of success of the RTS and, therefore, of the basic aspects of the new regulation of payment services in Europe, these ambitious objectives must be achieved.

Lack of agreement in this group would lead to a proliferation of divergent solutions that would enormously hamper both the implementation of the RTS and the harmonisation of payment services in the EU. If, on the other hand, the group successfully completes its work, the RTS will be an effective instrument to accommodate reasonably and adequately the significant biases and commitments imposed by the PSD2 and to ensure that the industry works together on matters that, apart from being fundamental to its daily operations, are strategic for its future.

3 The possible impact of the PSD2

Having analysed the main payment services digitalisation trends and the complexity of the PSD2, it is now time to evaluate the possible impact of these changes on the future structure and configuration of the market. Naturally, it is impossible to anticipate the precise scale of this transformation, especially when many of the regulatory changes still lack the necessary detail. However, it is possible to identify some underlying trends on the basis of which potential scenarios can be envisaged, along with their foreseeable implications for the different types of suppliers.

One of the characteristic features of the new digital environment for payment services is the increasing disconnect between payment account servicing and access to information on the transactions made with such account. The opening and servicing of payment accounts (mostly bank accounts) is a stringently regulated activity because, as public funds are involved, they have to be safeguarded. Traditionally, ASPSPs and the customer account holder have been the only parties to whom such transactions are visible, meaning that payment service provision required a direct commercial relationship between them. However, the popularisation of online payment solutions, based on card use and integrated into merchants' web portals, has contributed to weakening this link, although the underlying relationship remains very much present.

The application of the PSD2 can be expected to accentuate such disconnection, as it recognises the possibility of establishing an intermediary (a PISP) that interacts, on the customer's behalf, between the customer and the account-servicing payment service provider. AISPs will also be able to access customers' payment accounts and interact directly on their behalf with diverse entities.

As mentioned in the preceding section, the consequence of this regime is that intermediate entities may now establish a direct relationship with customers, thereby gaining access to data of undoubted commercial value, without having to bear the burden associated with the servicing of payment accounts, such as infrastructure maintenance and improvement, consumption of own funds, IT security costs, regulatory compliance, etc. This asymmetry seeks to foster competition within the payments industry and, as a result, its efficiency and

modernisation, but it needs to be scrutinised to avoid situations in which intermediate entities have unjustified competitive advantages.

This system of openness to authorised third parties is, in turn, the cause of a potential conflict between the growing interest in improving the protection of personal data (something the PSD2 reflects in its provisions on security) and the aspiration of fostering innovation and competition in the payment services space. Both banks and other payment service providers are obliged to comply with increasingly stringent data protection rules[25] and with the requirements arising from the PSD2 and its implementing regulations. Accordingly, there is a clear need to ensure that information of a personal nature supplied by an account-servicing payment services provider to a PISP or an AISP is treated securely and that data protection regulations are fulfilled.

In this context, in their account-servicing role, banks point to serious difficulties in being able to establish the necessary safeguards to ensure that third parties treat such information on the terms requested by customers. Among other reasons, this is because of the lack, as mentioned above, of a direct contractual framework between the parties that clearly defines their obligations. Given the responsibilities of ASPSPs arising from data protection regulations, the industry is thus exposed to a highly complex situation, necessitating a detailed analysis of its implications, possible guidelines and the cooperation of the various competent authorities.

Finally, the information-sharing regime advocated by the PSD2 is still rather asymmetric. The directive establishes that information on payment accounts should be accessible to third parties, although it confines its storage, consultation and use exclusively to the provision of the payment service envisaged (i.e. in the terms in which the latter is regulated). That said, the directive does not prevent, with the customer's explicit consent and irrespective of the payment service concerned, the simultaneous collection of this same information for other purposes.

Also, insofar as third-party providers do not, in turn, service payment accounts (as is the case of AISPs), they are under no obligation whatsoever to share with ASPSPs or any other interested third party the content of their respective databases.[26] This lack of reciprocity may, in turn, lead to greater concentration of the "market for data" owing to the presence of economies of scale and network effects in this area. Consequently, the tensions generated by this situation will foreseeably force a discussion in future as to whether similar rules to those of the PSD2 should be established in other areas unrelated to payment services. Until this occurs, the scenario described above may lead to competitive disadvantages for ASPSPs vis-à-vis other suppliers.

As mentioned, it is difficult to anticipate clearly the implications of the PSD2, although some preliminary comments can be made, taking into account the heterogeneity of the various types of supplier, which we have so far referred to as predominantly homogeneous groups.

---

25 The basic legislation is Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC.

26 This is particularly important in the case of large technology businesses that have chosen to operate as AISPs and that have a large customer database and extensive commercial information on their customers to be expanded on the basis of these new inputs.

Considering, first, account-servicing payment service providers (ASPSPs), banks clearly have a hegemonic position in this group, although it seems that not all banks are reacting in the same way to the PSD2 changes. Some traditional banks,[27] especially the small and medium-sized ones, will foreseeably not change their competitive behaviour and will react passively to the PSD2, introducing only those changes essential for compliance with the directive. This type of bank will restrict itself to transmitting to authorised third parties the payment account information that their customers wish to hand over to these new suppliers. It seems likely that these banks will not develop a specific API to facilitate the data transfer, but will allow the electronic banking channel they offer to their customers to be used.

On the other hand, other banks, possibly the largest and the recently created ones (internet banks without branches), may see the PSD2 as an opportunity. In consequence, although they will be ASPSPs vis-à-vis third parties, as required by the directive, they may also consider the possibility of acting as authorised third parties to obtain account data or to initiate payments in the accounts of their customers (old and new) at other banks. As ASPSPs, they will foreseeably develop dedicated interfaces, based on APIs, to improve the security and efficiency of data transmission. Conceivably, too, this type of bank will strive more to improve the on-line payment experience, adapting its communication interfaces with customers and successfully maintaining its links with them.

As for providers of payment initiation or account information services (TPPs), even greater heterogeneity is discernible, with three major categories distinguished. First, there would be small companies dedicated solely to providing payment initiation or account information solutions. The greatest challenge and limitation for this type of entity will foreseeably be the initial lack of a customer database, which may mean that they base their business model on providing a specific service or a specific technological solution covering specific gaps in the market.

Second, it is possible that large technology businesses (sometimes known as Big Tech), with a broad customer base and an extensive catalogue of non-financial services, may show interest in acting as account information service providers or payment initiators. The cost of obtaining a licence to provide account information services would be minor for these companies and, in exchange, would allow them to combine the considerable data they already have on their customers' tastes and preferences with financial data on their payment accounts. The latter, combined with the use of advanced analytical techniques, could help widen and improve the range of products and services offered to their customers, including, moreover, the experience of payment on their platforms when they choose to apply for a licence as a PISP. In this case, the provision of payment services could be the first step towards growing involvement in financial services.

Finally, as already noted, it should be borne in mind that there is no restriction on banks themselves acting as providers of account information or payment initiation services. In principle, banks may provide these types of services to try and retain and boost the loyalty of their customers, but also to gain market share, attempting to win customers from other banks.

The interactions between these groups of ASPSPs and TPPs will necessarily be complex, and it is difficult to anticipate the final scenario when there is still no clarity on some

27 Those other than digital banks, set up specifically to operate via the internet (also known as challenger banks).

important aspects of the PSD2. The final outcome will depend on diverse factors such as the nature of each country's banking structure, the appetite for innovation of its banks, the number and size of the banks interested in entering the market as authorised third parties, the loyalty of bank customers and, where applicable, the possible regulatory response.

In any case, the most likely outcome is that a situation will arise in which some banks will adapt and be capable of prospering in the new environment, while others have difficulty maintaining a fluid relationship with their customers. As regards new entrants (small start-ups), given the challenge posed by their limited customer base, they may form alliances with banks. However, the large technological platforms are the big unknown in this equation. If they are capable of harnessing the opportunity before them, these emerging actors will be called upon to be the main competitive threat to traditional banks, with a serious potential to transform the financial sector as hitherto known.

4 Conclusions

Today, the rate and depth of financial innovation are closely linked to the intensive application of new technologies, both as regards the design and provision of typical banking products and services, and how the processes and procedures needed for their marketing and support are organised and implemented.

The payment services industry has, so far, been the most visible outlet for most of these changes. Even so, this may still be the area liable to see the most far-reaching changes in the immediate future. With the PSD2 as prime example, the regulator has not wished to limit the competitive pressures currently on the industry, but, on the contrary, to enable broad access, by authorised third parties, to payment accounts that have been serviced mainly by banks.

Hence the use of customer information, the strategic nature of which remains intact, ceases to be an exclusive prerogative of banks, becoming – with the appropriate guarantees – more universal, and benefiting the customers themselves and society as a whole.

A scenario of uncertainty is opening up for traditional banks. As on many occasions in the past, they will have to find the most appropriate formula to mitigate the risks associated with the new reality and to make the best possible use of the major opportunities offered. The biggest challenges for banks are redefining business models and cooperating with new agents, along with the potential threat from big tech. These factors will set the pace of change, which will, without a doubt, leave a profound mark on the financial services markets.

Glossary of terms

AIS: Account Information Service

AISP: Account Information Service Provider

API: Application Programming Interface

AS-PSP: Account-servicing Payment Service Provider

B2C: Business-to-Consumer

CSC: Common and Secure Communication

ERPB: Euro Retail Payments Board

PIS: Payment Initiation Service

PISP: Payment Initiation Service Provider

PSD1: Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market, amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC

PSD2: Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC

PSP: Payment Service Provider

RTS: Regulatory Technical Standards

SCA: Strong Customer Authentication

TPP: Third-Party Provider

TRA: Transaction Risk Analysis

REFERENCES

AUTORIDAD CATALANA DE LA COMPETENCIA (2017). S*istemas de Pago,* No. 16/2017, Barcelona.

BBVA RESEARCH (2015). «PSD2, perspectiva del modelo de negocio: las API financieras fomentarán la innovación en el modelo de negocio», *Situación Economía Digital,* diciembre.

BRODSKY, L., and L. OAKES (2017). *Data sharing and open banking,* McKinsey & Company Financial Services, London and San Francisco.

CAPGEMINI (2018). *World FinTech Report.*

CARBÓ VALVERDE, S., and F. RODRÍGUEZ FERNÁNDEZ (2017). «Proyecciones de la digitalización financiera en España, 2017-2020», *Cuadernos de Información Económica,* septiembre.

COMISIÓN EUROPEA (2018). *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.*

KPMG (2017). *El nivel de madurez digital del sector financiero en España.*

PARLAMENTO EUROPEO Y CONSEJO (2015). *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010, and repealing Directive 2007/64/EC.*

– (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).*

SANTAMARÍA, J. (2018). *La Segunda Directiva de Servicios de Pago y sus impactos en el mercado,* Fundació Caixa d'Enginyers, Nota Técnica No. 31, enero.