EUROPEAN
COMMISSION

Brussels, 28.6.2023
COM(2023) 365 final

REPORT FROM THE COMMISSION

TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN CENTRAL BANK AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE

on the review of Directive 2015/2366/EU of the European Parliament and of the Council on payment services in the internal market

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN CENTRAL BANK AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE

on the review of Directive 2015/2366/EU of the European Parliament and of the Council on payment services in the internal market

Contents

ABBREVIATIONS

AIS	Account information service
AISP	Account information services provider
API	Application programming interface
ASPSP	Account servicing payment service provider
ATM	Automatic teller machine
DORA	Digital operational resilience act
EBA	European banking authority
EDIW	European digital identity wallet
ECB	European central bank
EEA	European economic area
EMD	Electronic money directive
EMI	Electronic money institution
GDPR	General data protection regulation
IBAN	International bank account number
IP	Instant payment
MIT	Merchant-initiated transaction
MOTO	Mail order or telephone order
NCA	National competent authority
OB	Open banking
OF	Open finance
PI	Payment institution
PISA	Payment instruments schemes and arrangements
POS	Point of sale
PSD2	Second payment services directive
PSP	Payment service provider
PSU	Payment service user
RPS	Retail payments strategy
RTS	Regulatory technical standard(s)
SCA	Strong customer authentication
SEPA	Single euro payments area
SFD	Settlement finality directive
TMM	Transaction monitoring mechanism(s)
TPP	Third party provider
TSP	Technical service provider

1. INTRODUCTION

The second Payment Services Directive (PSD2[1]) provides a framework for all retail payments in the EU, euro and non-euro, domestic and cross-border. The first Payment Services Directive (PSD1[2]), adopted in 2007, established a harmonised legal framework for the creation of an integrated EU payments market. Building on PSD1, PSD2 addressed barriers to new types of payment services and improved the level of consumer protection and security. The review clause of PSD2 (Article 108, see Appendix 1) required the Commission to report on the application and impact of PSD2 by 13 January 2021 in particular on charges, scope, thresholds and access to payment systems. The review could not take place by that date due to the directive's late transposition by some Member States and the delay in applying some of its rules, such as on Strong Customer Authentication (SCA, see §3.4 below)[3]. The evaluation of PSD2 therefore only took place in 2022[4]. Following the evaluation, and in light of its 2020 Communication on a Retail Payments Strategy (RPS) for the EU[5], the Commission decided to revise PSD2. The present review report accompanies the two legislative proposals revising PSD2.[6]

2. APPLICATION AND IMPACTS OF PSD2 IN GENERAL

Recent years have seen many changes in the payment services market. Electronic payments in the EU have been in constant growth, reaching €240 trillion in value in 2021 (compared with €184.2 trillion in 2017)[7]. Alongside the increasing use of cards, new providers enabled by digital technologies have entered the market. For example, non-bank payment service providers (PSPs) such as payment institutions (PIs) and e-money institutions (EMIs) are now widely present. Open banking services, including account information and payment initiation services, have significantly grown over this period (see §3.1 below).

The PSD2 evaluation report concludes that PSD2 has had varying degrees of success in meeting its objectives. One area of clear positive impact has been that of fraud prevention, via the introduction of SCA; although more challenging to implement than anticipated, SCA has already had a significant impact in reducing fraud. PSD2 has also been particularly effective with regard to its goal of increasing the efficiency, transparency and choice of payment instruments for payment service users. However, the evaluation found that there are limits to PSD2's effectiveness in achieving a level playing field, most notably the persisting imbalance between bank and non-bank PSPs resulting from the lack of direct access by the latter to certain key payment systems. In spite of the emergence of hundreds of new non-bank providers servicing millions of clients, there has been mixed success in the uptake of open banking (OB) in the EU, with issues relating to the performance of data access interfaces for OB service providers. While cross-border provision of payment services is increasing, many payment systems (especially debit card systems) remain largely national. No new fully pan-European payment solution has yet emerged. The European Payments Initiative (EPI)[8] is

[1] Directive (EU) 2015/2366 of 25 November 2015 on payment services in the internal market.
[2] Directive 2007/64/EC of 13 November 2007 on payment services in the internal market.
[3] Most of the rules in PSD2 have been applicable since January 2018, but those on SCA have applied only since September 2019.
[4] The Evaluation Report can be found at Annex 5 of the Impact Assessment, SWD 2023/231 final. The evaluation was partly based on a report by a contractor, VVA/CEPS, which is available at this link.
[5] COM/2020/592 final, of 24/9/2020.
[6] COM (2023) 366 final and COM(2023) 367 final.
[7] ECB, Statistical Data Warehouse, Payments Statistics Report, July 2022.
[8] See https://www.epicompany.eu/.

currently developing its first pan-European payment solution. Anticipated cost reductions for merchants from new cheaper payment means, for example based on OB, have not yet fully materialised. Overall, the evaluation concludes that despite certain shortcomings the current PSD2 framework has enabled progress towards its objectives.

These and other issues are treated in more detail in section 3 below, which includes the issues highlighted in article 108 of PSD2 and summarises the outcome of the review of PSD2 more generally.

3. SPECIFIC ASPECTS OF PSD2

3.1. Open banking

Open banking (OB) is the term given to the process by which account information service providers (AISPs) and payment initiation service providers (PISPs), collectively known as third party providers (TPPs), provide or facilitate PSD2-regulated services to users based on accessing – upon user request - their account data held by account servicing payment service providers (ASPSPs). Although open banking existed in the EU before PSD2, TPPs operated in a largely unregulated environment. PSD2 gave OB a stable regulatory framework, with safeguards for users. It imposed an obligation on ASPSPs to facilitate TPP access to payments data without any mandatory contractual obligations, with the objective of stimulating the development of OB, while laying down measures to provide greater security and protection to users.

While a growth trend in OB could already be observed prior to PSD2, the market in OB services has continued to grow since 2018. The number of TPPs and users of OB services in the EU has been increasing, reaching almost 19 million users in 2021.[9] The legal framework has legitimised TPPs' regulated access to payment accounts and the security of users and of their data has been ensured. However, the PSD2 evaluation has revealed recurrent problems as regards effective and efficient access by TPPs to data held by ASPSPs. TPPs still face substantial obstacles and frequently report that the interfaces which have been designed to facilitate their data access[10] vary in quality and performance. ASPSPs report significant implementation costs for the development of APIs[11] and regret that the legislative framework of PSD2 prevents them from charging TPPs for facilitating access to customer data via APIs. ASPSPs also often express dissatisfaction with the low use of their APIs by TPPs and the continued use by some TPPs of their customer interface rather than of the API.

Against this background, the choice made by the Commission following the PSD2 review is to make a number of targeted amendments to the OB framework to improve its functioning, but to avoid radical changes which might destabilise the market or generate significant further implementation costs. Despite the existence of different API standards in the EU[12] the Commission deems it preferable not to impose a new fully standardised EU data access interface. Doing this would present some obvious advantages in terms of data access by TPPs. Adapting to a new standard would however be quite costly for the market as a whole. The PSD2 API standards in place in the EU, whilst still presenting some differences, have substantially converged over time. And one of the two main API standards claims to account

[9] Figure from Juniper research, cited by Statista. There are no official statistics on open banking in the EU.
[10] Usually APIs, as the vast majority of ASPSPs opted for an API as open banking interface.
[11] According to a report by the Commission contractor VVA/CEPS, over €2 billion in one-off implementation costs.
[12] There are essentially two main PSD2 API standards in the EU (the 'Berlin Group' standard and the 'STET' standard).

for 80% of the European open banking APIs.[13] In addition, although differences subsist (often caused by individual ASPSP variations of the main standards), API "aggregators" provide a single implementation point, allowing the simultaneous connection by TPPs to a multitude of different APIs. Therefore, the Commission, largely supported by the market, considers that the costs of introducing a new single API standard in the EU would overall outweigh the benefits.

Nor does the Commission see merits in changing the PSD2 default rule of allowing access to data by TPPs without a mandatory contractual relationship and therefore without financial compensation for ASPSPs. Introducing such a radical change in the open banking ecosystem would be potentially very disruptive, with no guarantee that the performance of interfaces would be rapidly and significantly improved. The market should however be free to conclude agreements, accompanied by a compensation regime, for services going beyond those regulated in the revised PSD2,[14] but it should always be possible for any TPPs to benefit from the PSD2 'baseline' services without prior contractual agreement or charging. On the other hand, new minimum requirements for the performance of dedicated interfaces, including a non-exhaustive set of prohibited OB obstacles, will be laid down in the acts revising PSD2 to ensure optimal TPP data access for the full benefit of their clients.

Currently, with PSD2, ASPSPs must maintain -except if they benefit from an exemption- two OB data interfaces, a principal interface and a "fallback interface". However, this rather complex regime should be streamlined: if ASPSPs offer compliant dedicated interfaces providing to TPPs the data they need to service their clients, there is no reason to continue with this two interfaces requirement. ASPSPs should rather only be required to maintain permanently one "dedicated" OB interface.[15] But the removal of the permanent fallback interface, which many TPPs still often use given the suboptimal quality of certain APIs, must indispensably be accompanied by a substantial upgrade of the interfaces performance level and a robust enforcement regime. These are two indispensable prerequisites to the simplification of the current landscape and the abandonment of the requirement of maintaining a permanent "fallback" interface. However, even if of high quality, APIs may sometimes break down and TPPs must, in these circumstances, be offered a means of preserving business continuity through temporary contingency data access. Finally, to increase consumers' trust in OB and facilitate their use of OB services and to improve consumer protection, banks and other ASPSPs will be required to offer to their clients making use of OB services an IT tool (a "dashboard") allowing them to see at a glance what data access rights they have granted and to whom and, should they desire, to cancel TPP access to their data via this tool.

Together with the two proposals revising PSD2 the Commission is presenting a legislative proposal on financial information data access (FIDA), extending the obligation to provide access to financial data beyond payment account data ("Open Finance"). The Commission examined the possibility of transferring AISPs from PSD to the future FIDA framework. Although such a transfer could ultimately make sense, given the nature of AISPs' business, there would be a significant risk of disruption and data access rights interruptions for AISPs if such a transfer were to be carried out prematurely, i.e. before the existence of a "scheme",

[13] PRESS RELEASE - Berlin Group is offering support to new European payment schemes (berlin-group.org)

[14] Such as for example the SEPA Payment Account Access Scheme currently discussed by the market. SEPA Payment Account Access | European Payments Council

[15] Except where, on proportionality grounds, their supervisory authority grants them a dispense from having a dedicated interface in light of their business model.

which will be a pre-requisite for Open Finance to take place[16]. There is currently no such scheme in the OB market, although one is currently being designed by market participants. It is therefore deemed preferable by the Commission to have a staged approach and provide for such a transfer when the FIDA framework is fully operational and only if and when the conditions for a smooth transfer are considered appropriate.

3.2. Scope[17]

New means of payment have been developed since PSD2 was adopted, such as instant payments or e-money tokens (EMTs, a type of crypto asset[18]). Other new products are e-wallets (specifically "pass-through wallets") which allow, through tokenisation, the use of a payment instrument via a mobile device to make online or contactless payments. New services facilitating the provision of payment services without themselves being payment services, such as "buy-now-pay-later" or "request-to-pay", have also emerged.

Many providers of such new services are excluded from the scope of PSD2 as being "technical service providers" (TSPs). These include payment system operators and service providers such as payment processors or gateways which, although not PSPs themselves, support the provision of payment services by regulated PSPs. Some of these TSPs have, since PSD2, gained a very significant role in the payment chain and some of them, like big payments data processors, have even acquired quasi-systemic status in some Member States. This situation may obviously generate new risks in the EU payments landscape.

Against this background, the Digital Operational Resilience Act (DORA) is relevant[19]. PSPs in the meaning of PSD2 are included within the scope of DORA whose provisions apply directly to them. However, payment system operators, which are not currently subjected to a licensing regime under PSD2[20], fall outside the scope of DORA as DORA only applies to financial entities which are regulated and supervised under EU legislation. DORA mandated the Commission, in the context of the PSD2 review, to consider the inclusion of *"operators of payment systems and entities involved in payment–processing activities"* within the scope of PSD2, which would consequently allow their inclusion within the scope of DORA[21].

The Commission has reached the conclusion that such inclusion would, at this stage, be premature. There is no prevailing view on this question among stakeholders - whether private or public - consulted by the Commission during its PSD2 review, and no clear detriment or risk to consumers or other market players has yet been observed. Many of the currently excluded services and their providers are already - or are about to be - subjected to European Central Bank/Eurosystem oversight (based on article 127§2 of the Treaty). Schemes and so-called "arrangements" (such as digital wallets) are covered by the new 'PISA' oversight framework of the Eurosystem, which is currently being progressively rolled out. There would therefore be a significant risk of duplication if a new layer of EU supervision were to be added to the existing layer of ECB/Eurosystem oversight, without robust evidence of the need for it. Also, the main logic of PSD2 is to regulate services provided to end-users (consumers, merchants) and not services pertaining to the operation of payment infrastructures, nor

[16] See the Commission's proposal for a regulation on harmonised rules on fair access to and use of data (Data Act), COM(2022) 68 final of 23 February 2022.

[17] This section responds to article 58(2) of DORA; see Appendix 2.

[18] These are regulated, along with other crypto assets which are not suitable for use as a means of payment, in Regulation (EU) 2023/1114 of 31 May 2023 on markets in crypto-assets (MiCA).

[19] Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector.

[20] However one article of PSD2, article 35, does impose requirements on payment system operators.

[21] Article 58(2) of DORA. See Appendix 2.

services supporting the execution of payment services without being payment services themselves (for example payment data processing, operation of payment terminals, cloud services etc.) or services which only facilitate the use of a payment instrument, without any regulated payment service being involved. EU financial services legislation tends to separate consumer-related issues and regulation of wholesale and infrastructure issues in separate pieces of legislation[22].

The Commission is however fully aware of the growing importance of these unsupervised operators in the provision of payment services, and of the potential risks that their activities may potentially cause to payment systems and financial stability. The Commission will therefore, within 3 years of application of the revised legislation, carry out a thorough review, based on evidence and in close cooperation with the ECB/Eurosystem, assessing in particular whether a dedicated EU licensing and supervision regime for some of the hitherto excluded entities is necessary in addition to the existing oversight regime. This timescale is necessary in order to gather sufficient evidence of implementation.

In light of these considerations, the PSD2 revision proposal only makes essential clarifications on the rules on the scope of PSD2 where there are currently ambiguities, but without introducing significant changes to the existing PSD2 scope.

Access to cash is a Commission priority. The new proposal contributes to this goal by facilitating access to cash. Currently, under PSD2, a retailer may provide cash to a customer without a PSP license, but only in association with a purchase ("cashback"). In order to further increase access to cash the Commission proposes to allow retailers to offer a cash provision service even in the absence of a purchase by a customer, without having to obtain a PSP license or being an agent of a payment institution. This is associated with some conditions, such as a cap of €50[23] per withdrawal and an obligation to disclose any fees charged.

The distribution of cash via ATMs in general requires a PSP license, but there is an exclusion in PSD2 for certain non-bank ATM operators, with specific conditions[24]. This exclusion has proven difficult to apply in practice. It is therefore proposed to remove the exclusion, but to include in the scope ATM operators which do not service payment accounts with a lighter registration regime and an appropriate level of regulation (for example, transparency on fees will be required).

3.3. Consumer protection

i. Rules on charges[25]

PSD2 allows payees to impose charges on payers in order to steer them towards the use of specific payment instruments (so-called "surcharging"). However, payees are prevented from requesting charges for the use of payment instruments for which interchange fees are regulated under the Regulation on Interchange fees[26], i.e. for consumer debit and credit cards issued under four-party card schemes, and for those payment services to which the SEPA

[22] For example, MiFID (Directive 2014/65/EU of 15 May 2014 on markets in financial instruments) and the Regulation on Central Securities Depositories (Regulation (EU) No 909/2014) in the field of securities.

[23] Notably in order to preserve fair competition with ATMs and to prevent shops quickly running out of cash.

[24] Article 3(o) of PSD2.

[25] This section responds to article 108(a) of PSD2; see Appendix 1.

[26] Regulation (EU) 2015/751 of 29 April 2015 on interchange fees for card-based payment transactions.

Regulation[27] applies, i.e. credit transfers and direct debits in euro. Member States are currently allowed to ban or limit surcharging more widely, an option that has been used in more than half of Member States. The Commission considers that there is no need to further align or modify charging practices between Member States, as the surcharging ban already applies to 95% of payments in the EU. This conclusion is supported by most respondents to the public consultation. However, the surcharging ban in PSD2 does not currently extend to credit transfers and direct debits denominated in non-euro EU currencies. As there is no clear rationale for this restriction, the Commission is proposing to extend the surcharging ban to all credit transfers and direct debits in all currencies.

ii. Rules on transactions with third countries[28]

PSD2 applies to payment transactions within the EU and from and to third countries in any currency (including non-EU currencies); however, its provisions are limited to those parts of a transaction that are carried out in the EU. Fees and fee transparency for intra-EU payments are covered by the Regulation on cross-border payments[29], but that Regulation does not cover remittance transactions and credit transfers from the EU to third countries. When a currency conversion is necessary the costs related to this are often an important share of the total costs. For transactions from the EU to third countries, without full transparency on costs and fees it is hard for consumers to compare charges of different providers; consequently, they may choose a provider which is not the most suitable to their needs. In addition, under the current PSD2 there is no requirement for PSPs to give the payment service user an estimate of the maximum execution time for such transactions.

Promoting competition and reducing fees for international credit transfers and remittances is one of the objectives of the G20 Roadmap on cross-border payments[30]. Therefore, for credit transfers and money remittances from the EU to third countries, the Commission is proposing an obligation to inform the payment service user about the estimated charges for currency conversion, in line with current information requirements for intra-EU transactions, as well as the estimated time for the funds to be received by the payee's payment service provider in a third country. The Commission does not however propose to set a maximum time for the execution of credit transfers and transfers of funds from the EU to third countries, as this partly depends on banks outside the EU which are not subject to EU rules.

iii. Thresholds related to the exclusion of electronic communications networks[31]

PSD2 excludes from its scope payment transactions carried out by a provider of an electronic communication network that are carried out from or via an electronic device, or for purchase of digital content or voice-based services (e.g. ringtones, music and premium SMS-services), where the transaction is charged to the subscriber's bill. This exclusion is limited to EUR 50 per transaction and EUR 300 per month. The Commission did not identify, in its PSD2 review, any issues related to the current levels of the various thresholds set in PSD2. In view of the evidence received in its review, the Commission is not proposing changes to the thresholds but will continue to monitor their adequacy.

---

[27] Regulation (EU) 260/2012 of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro.

[28] This section responds to article 108(b) of PSD2; see Appendix 1. "Third countries" are to be understood as countries outside the European Economic Area.

[29] Regulation (EU) 2021/1230, containing transparency obligations for the estimated total amount and applicable currency conversion charges.

[30] https://www.fsb.org/wp-content/uploads/P131021-1.pdf.

[31] This section responds to article 108(d) of PSD2; see Appendix 1.

iv. Rules on blocking of funds[32]

When a payment card is used for a payment of an uncertain amount (for example at a petrol station, a hotel or a car rental), funds are normally blocked on the card by the payer's PSP after consent has been given by the payer. Blocked funds are unavailable to the user for spending until released, which can cause financial difficulties. Evidence shows that the blocked funds may be disproportionate or unreasonably high compared with the final amount, when known. The issue of excessive blocked amounts cannot be solved by introducing caps, as different situations may require very different blocked amounts (fuel purchase, car rental, hotel stay, etc.). This was echoed by a majority of stakeholders in the public consultation[33]. Another related issue concerns variations in the timing of release of unused blocked funds, which could, according to feedback received, take up to several weeks to be released or even require an explicit request from the payer. Against this background, the Commission is proposing changes to speed up the pay-out of unused blocked funds and to require that the blocked amount be proportionate to the expected final amount, rather than proposing the introduction of absolute maximum amounts.

3.4. Security and fraud prevention

In the area of fraud, the major innovation of PSD2 was the introduction of SCA. This involves two authentication factors based on either knowledge (e.g. a password), possession (such as a card) or inherence (such as a fingerprint). PSD2 requires PSPs to apply SCA where the payer accesses a payment account online, initiates an electronic payment transaction or carries out any action through a remote channel which may imply a risk of payment fraud or other abuses. The evaluation carried out by the Commission shows that SCA has already been highly successful in reducing fraud. For example, with regard to remote card payments, SCA-authenticated transactions have a 70-80% lower level of fraud than those without[34]. However, the progressive introduction of SCA by the market was challenging, causing some major delays to its full roll-out. Market participants regularly stress the costs incurred by the introduction of SCA[35] and many would prefer a more purpose-based approach in order to reduce SCA-related friction in electronic transactions. The Commission acknowledges that the introduction of SCA could have been smoother and could certainly have been better anticipated by the market, which largely underestimated the complexity and the impact of this migration. The Commission does not however intend to change its approach concerning SCA, given the very positive results that it has already had on fraud levels and the fact that, by now and after its progressive introduction, SCA has become familiar to most of its users.

The introduction of SCA posed some concrete challenges to many EU consumers, affecting their possibility to carry-out electronic payments. The Commission believes that everyone should be capable of performing SCA, irrespective of their health, age or condition. PSPs must therefore have in place means to perform SCA that cater for all their clients and not only those who, for example, possess a smartphone or are familiar with technology. The Commission will require PSPs to facilitate the use of SCA by, for example, persons with

[32] This section responds to article 108(f) of PSD2; see Appendix 1.

[33] The public consultation replies are available at this link.

[34] European Banking Authority, Discussion paper on EBA's preliminary observations on selected payment fraud data under PSD2, as reported by the industry, EBA/DP/2022/01, 17 January 2022.

[35] According to a report by the contractor VVA/CEPS, over €5 billion in one-off implementation costs, but offset by an annual reduction in fraud of almost €1 billion per year.

disabilities, older people, and others experiencing difficulties using SCA, in line with the European Accessibility Act.[36]

Despite its success SCA does not address all types of fraud. Faced with the emergence of new types of fraud, particularly "social engineering" fraud, in which fraudsters manipulate their victim to reveal their credentials or send funds to an illegitimate payee, for which SCA is on little effect, the Commission proposes new measures regarding both fraud prevention and redress[37]. These include improvements to the application of SCA (e.g. clarifications of when a transaction qualifies as merchant-initiated or a mail or telephone order), the creation of a legal basis for PSPs to share fraud-related information in full respect of GDPR, as universally requested by the market, an obligation by PSPs to carry out education actions to increase customers awareness of payments fraud and an extension to all credit transfers -not only instant payments- of IBAN/name verification services, which have already proven their efficiency against fraud and mistakes in those markets where they were introduced[38].

PSD2 introduced a refund right for consumers but only as regards unauthorised credit transfers, i.e. those where the payer has not consented to the execution of the payment transaction. It does not however cover the types of fraud which have emerged since its adoption and which have become increasingly widespread, such as social engineering fraud mentioned above. While the application of SCA introduced by PSD2 has already led to a significant reduction in the level of fraud related to unauthorised payment transactions, it is largely inefficient in preventing these new types of fraud. The Commission considers that, with social engineering, the difference between authorised and non-authorised transactions is becoming more blurred and complex to apply in practice, raising also legal questions as to whether a transaction can be deemed authorised just because SCA was performed.

The Commission believes that any changes to the PSD2 liability framework should contribute to reducing fraud but without creating a new moral hazard, which a general refund right could create, or simply reallocating the financial consequences of fraud. It therefore proposes to introduce additional refund rights for consumers beyond for unauthorised transactions, but only for some specific situations - and subject to some conditions. The logic followed by the Commission is that where, because of its actions or inactions, the payment service provider's liability can be considered as engaged a refund right may be justified. One of these situations is where the consumer suffered damages caused by a failure of the IBAN/name verification service. Another situation where a refund right would be warranted is where a consumer is victim of a fraud where the fraudster pretends to be an employee of the consumer's bank, for example using the bank's telephone number or e-mail address ("impersonation fraud", or "spoofing"). In this latter case the PSP, having had its credentials and staff fraudulently usurped, could be considered as a victim as well, like the consumer. However, in a growing number of Member States banks, rightly concerned by the impact of such fraud of their reputation and on consumers' trust in the banking system, increasingly choose to refund such fraudulent "spoofing" transactions. Some national court rulings seem to follow the same trend. It is however indispensable to have some exceptions and safeguards to such refund

[36] Directive 2019/882 of 17 April 2019 on the accessibility requirements for products and services.

[37] Commission services have estimated the value of social engineering fraud at €323 million per year, on the basis of EBA data. See the impact assessment accompanying the Commission's proposal on instant payments, SWD(2022)546 final.

[38] Such services, which exist at domestic level in certain Member States, alert a payer before a payment is finalised of any discrepancy between the account number (IBAN) and the name of the payee. An obligation on PSPs to offer such a system is already proposed (but only for instant credit transfers in euro) by the Commission's legislative proposal on instant payments (COM(2022) 546 final of 26/10/2022).

rights, in particular where there is gross negligence by the consumer or where the consumer is part of the scam.

The Commission accords utmost importance to the issue of fraud. It will closely monitor the evolution of payment fraud, in cooperation with consumer organisations, and will be ready, should it become necessary, to propose adjustments to the legal framework, including on further broadening the shift of liability. The Commission expects every actor of the payment chain, private or public, regulated or not, to play its full part in fraud prevention. Merchants, payment schemes, technical services providers, mobile network operators, internet platforms and others should fully play their part in the collective effort alongside the regulated PSPs, and their liability could in some situations be engaged as well.

3.5. De-risking and competition-related issues[39]

Non-bank PSPs have grown in numbers and importance since the entry into force of PSD2. Although they can offer payment account services, unlike banks they may not lend and they must safeguard customer funds with a commercial bank in order to obtain a license. PIs and EMIs thus need to have an account with a commercial bank. Furthermore, offering payment services requires access to key payment infrastructures that process and settle payments.

Problems of 'de-risking' by commercial banks have been encountered by PIs and EMIs, as evidenced by the EBA in its January 2022 Opinion.[40] With regard to access to commercial bank accounts, although banks are required by PSD2 to explain and justify any refusal to grant account access to a PI or EMI, they often give superficial pro-forma explanations for doing so, or else grant access but subsequently withdraw it, which PSD2 does not require them to explain. This can cause major disruption to the activity of PIs and EMIs.

Furthermore, the Settlement Finality Directive (SFD[41]), as it stands, prevents access by non-bank PSPs to payment infrastructures which have been designated by Member States under that Directive, by not mentioning them as possible participants. This forces PIs and EMIs to rely even more on commercial banks, not only for safeguarding of customer funds but also for execution of payments, establishing a structural dependency of non-bank PSPs on banks and an unlevel playing field denounced by numerous market participants.

The Commission's proposal revising PSD2 therefore contains measures to remedy these failings and make the playing field more level. Requirements on banks regarding bank account services to non-bank PSPs will be considerably toughened, with a stronger requirement to explain refusal, covering also, unlike in PSD2, withdrawal of service. Central banks will also be allowed to provide account services to non-bank PSPs, at their discretion. The Commission is also proposing to amend SFD to include PIs[42] as possible participants in designated payment systems. The revised payment rules will include reinforced rules on the admission of PIs as participants in payment systems, with appropriate risk assessment.

3.6. Enforcement

Adequate enforcement is essential to ensure harmonised application and implementation of PSD2 rules. The full harmonisation principle requires Member States not to maintain or introduce provisions other than those laid down in PSD2. PSD2 rules are however differently

[39] This section responds to article 108(c) of PSD2 ; see Appendix 1.

[40] EBA Opinion and annexed report on de-risking.pdf (europa.eu)

[41] Directive 98/26/EC of 19 May 1998 on settlement finality in payment and securities settlement systems, as amended.

[42] Not EMI as the status of e-money institution will be combined with that of payment institution in the future framework; see §3.7(ii) below.

interpreted and implemented by the various stakeholders in the payments market, despite the fact that there is interpretative non-binding guidance available, inter alia, in the framework of the Question-and-Answer tool, Opinions and guidelines of the EBA.[43] Supervision of PIs is conducted along national lines with national competent authorities responsible within their jurisdiction. An unlevel playing field with potential for regulatory arbitrage exists where PSPs establish themselves in a Member State that applies PSD2 rules in a way that is advantageous for them and from there carry out cross-border services to other Member States with stricter interpretations.

Against this background, it is appropriate to strengthen the enforcement powers of national competent authorities, in particular in the field of penalties, and to ensure uniform application of EU rules on payments by transforming the greater part of the rules in PSD2 into a directly applicable Regulation.

3.7. Other issues

i. Smaller payment institutions[44]

PSD2 allows Member States to subject smaller PIs to lighter supervisory requirements, provided that certain thresholds regarding executed payment transactions are respected[45]. No substantial issues related to the current level of the thresholds have been identified, and therefore there is no compelling reason for the Commission to propose changes to the thresholds; however, the Commission proposes to update the thresholds for inflation and to do so periodically in future, using delegated legislation.

ii. Simplification: streamlining with e-money services

The second E-Money Directive (EMD2[46]) contains rules on authorisation and supervision of e-money institutions (EMIs). PSD2 contains rules on authorisation and supervision of PIs and establishes rights and obligations and transparency requirements in the relationship between all payment service providers (including EMIs) and payment service users. As payment transactions using e-money are already regulated to a very large extent by PSD2, the legal framework applicable to EMIs and PIs is already reasonably consistent. However, the licensing requirements, in particular initial capital and ongoing capital, and some key concepts governing the e-money business, such as issuance of e-money, e-money distribution and redeemability, are quite distinct as compared to the services provided by payment institutions. Supervisory authorities have experienced practical difficulties in clearly delineating the two regimes and in distinguishing e-money products/services from payment services offered by PIs. This has led to concerns about regulatory arbitrage and an unlevel playing field, as well as to issues with possible circumvention of the requirements of EMD2 whereby some institutions issuing e-money, taking advantage of the similarity between payment services and e-money services, apply for authorisation only as a payment institution.

The experience acquired is now sufficient to conclude that a merger of the two regimes[47] is appropriate, bringing them together in one single piece of legislation and harmonising them to the extent possible, while still leaving room for specificities where justified. This will address

[43] Single Rulebook Q&A | European Banking Authority (europa.eu)
[44] This section responds to article 108(e) of PSD2; see Appendix 1.
[45] Article 108(e) in conjunction with article 32 of PSD2.
[46] Directive 2009/110/EC of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions, as amended.
[47] See the Commission report on the implementation and impact of Directive 2009/110/EC, in particular on the application of prudential requirements for E-Money Institutions.

concerns and challenges with regard to delineating the two legal frameworks, in particular at the licensing stage. It will furthermore ensure a higher degree of harmonisation, simplification and consistent application of the legal requirements for PIs and EMIs, preventing regulatory arbitrage, ensuring a level playing field and a future-proof legal framework.

4. CONCLUSIONS

In light of the results of the evaluation report on PSD2, the Commission concluded, on the one hand, that targeted amendments are necessary and timely but, on the other hand, that those amendments should represent an evolution but not a revolution for the EU payments framework. In certain areas – for example the scope of the legislation or surcharging – no evidence was found of problems that would justify major and immediate changes, although this will be kept under review, especially as regards operators of payment systems in light of the review clause of DORA. In other areas, for example open banking, considering the legacy that PSD2 represents and the investments already made to implement the PSD2 standards, and the costs that profoundly changing such requirements would entail, the Commission deems it essential to discard any options associated with significant new implementation costs and/or uncertain outcomes.

The proposed revisions to PSD2 represent a package of changes which will enhance the functioning of the EU payments market and substantially reinforce consumer protection. These changes are fully in line with the objectives of the Commission's retail payments strategy and complementary to ongoing initiatives such as the legislative proposal on instant payments and the proposal on "open finance" (FIDA) which the Commission is also proposing with its PSD2 revisions.

APPENDIX 1

Article 108 of Directive (EU) 2015/2366

Review clause

"The Commission shall, by 13 January 2021, submit to the European Parliament, the Council, the ECB and the European Economic and Social Committee, a report on the application and impact of this Directive, and in particular on:

(a) the appropriateness and the impact of the rules on charges as set out in Article 62(3), (4) and (5);

(b) the application of Article 2(3) and (4), including an assessment of whether Titles III and IV can, where technically feasible, be applied in full to payment transactions referred to in those paragraphs;

(c) access to payment systems, having regard in particular to the level of competition;

(d) the appropriateness and the impact of the thresholds for the payment transactions referred to in point (l) of Article 3;

(e) the appropriateness and the impact of the threshold for the exemption referred to in point (a) of Article 32(1);

(f) whether, given developments, it would be desirable, as a complement to the provisions in Article 75 on payment transactions where the amount is not known in advance and funds are blocked, to introduce maximum limits for the amounts to be blocked on the payer's payment account in such situations.

If appropriate, the Commission shall submit a legislative proposal together with its report."

APPENDIX 2

Article 58(2) of Regulation (EU) 2022/2554 (DORA)

"In the context of the review of Directive (EU) 2015/2366, the Commission shall assess the need for increased cyber resilience of payment systems and payment-processing activities and the appropriateness of extending the scope of this Regulation to operators of payment systems and entities involved in payment-processing activities. In light of this assessment, the Commission shall submit, as part of the review of Directive (EU) 2015/2366, a report to the European Parliament and the Council no later than 17 July 2023.

Based on that review report, and after consulting ESAs, ECB and the ESRB, the Commission may submit, where appropriate and as part of the legislative proposal that it may adopt pursuant to Article 108, second paragraph, of Directive (EU) 2015/2366, a proposal to ensure that all operators of payment systems and entities involved in payment-processing activities are subject to an appropriate oversight, while taking into account existing oversight by the central bank."