A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2)

FISMA/2021/OP/0002

A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2)

FISMA/2021/OP/0002

Authors:

VVA: Ivan Bosch Chen, Davide Fina, Pierre Hausemer, Andrej Henžel, Christian Neumann, Nelly Patroclou, Charu Wilkinson.

CEPS: Willem Pieter De Groen, Tamás Kiss-Galfalvi, Jelmer Nagtegaal, Inna Oliinyk, Meryen Gökten, Fredrik Andersson, Beatriz Pozo, Agustina Korenblit, Tobias Lannoo.

With the support of: Mariachiara Malaguti (Catholic University of the Sacred Heart), Antonella Sciarrone (Catholic University of the Sacred Heart), Michał Polasik (Nicolaus Copernicus University in Torun).

EUROPEAN COMMISSION

Directorate-General for Financial Stability, Financial Services and Capital Markets Union
Directorate B — Horizontal Policies
Unit B.3 — Retail financial services

FISMA-PSD2-REVIEW@ec.europa.eu

European Commission
B-1049 Brussels

A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2)

FISMA/2021/OP/0002

LEGAL NOTICE

PDF ISBN 978-92-76-62087-7 doi 10.2874/996945 EV-04-23-061-EN-N

Luxembourg: Publications Office of the European Union, 2023

Abstract

This study contributes to the review of the Directive (EU) 2015/2366 on Payment Services (PSD2) by assessing whether the introduction of the PSD2 helped reach the five general objectives identified in the European Commission's impact assessment. To do this the study analyses the key trends that have affected the payments market and the performance of the Directive in terms of its relevance, effectiveness, efficiency, coherence and EU added value. Based on the conclusions of this assessment, the report identifies a number of areas where there is room for improvement and it provides a set of recommendations regarding possible revisions of PSD2 provisions. From a methodological perspective, the assessment is supported by a comprehensive review of literature on market trends, in-depth legal research in selected EU Member States, and primary fieldwork through interviews and an online survey. Following the Commission's Better Regulation Guidelines, the analysis is based on an evaluation framework and underpinned by a cost-benefit analysis.

Table of Contents

Table of Annexes

List of Tables

List of Figures

Executive Summary

This is the Final Report for the Study on the Application and Impact of Directive (EU) 2015/2366 on Payment Services (PSD2). The study contributes to the review of the Directive (EU) 2015/2366 on Payment Services (PSD2) through:

- a comprehensive assessment of the implementation and application of the PSD2; and
- a set of recommendations on possible revisions to PSD2 provisions.

To answer the research questions, primary and secondary data was collected via:

- desk research (including policy and market research in all EU Member States and beyond and legal research in a sample of 10 Member States; and
- stakeholder interviews and online survey covering policy makers, national authorities, market players and consumer organisations. Inputs were collected from 266 stakeholders representing all EU Member States.

The analysis was guided by the intervention logic of the PSD2 and an evaluation matrix setting out the approach to addressing the key research questions. The conclusions of the study are based on an in-depth qualitative assessment of all the collected information as well as a quantitative model of the costs and benefits of the PSD2.

Market trends

Trends in the payments market since implementation of PSD2

In recent years, European retail payments markets have undergone a significant transformation including an increasing availability of new digital contactless payments methods, and increasing usage of third-party payment initiation and account information aggregation services.

While cash remains popular, there is an irreversible trend towards cashless payments. Cash is still the most accepted payment method at points of sale (POS) but it is increasingly used only for lower value day-to-day transactions or where it is the only accepted payment method. Indeed, since 2007, cash usage in POS retail payments has been declining[1] and it has been replaced by cards and other electronic payment methods.

Payment cards are the most popular means of cashless payments in almost all Member States. Decreasing merchants' cost of accepting cards as well as the Covid-19 pandemic have accelerated card usage at POS. However, the adoption of contactless cards and card-based mobile wallets varies across Member States.

Several new alternatives to online card payments have emerged in recent years. When it comes to e-commerce more specifically, online bank transfers currently represent the most preferred alternative to card-based online payments. In addition, digital wallets which are used for both in-store and online payments, such as PayPal and Apple Pay, have seen an increase in popularity in recent years.

There is growing demand for better cross-border payment solutions. Although a well-functioning cross-border payment infrastructure plays a crucial role for the integration of the EU economy, cross-border payments have often been slow, inefficient, and costly for banks and merchants. The rise of online market platforms, such as Amazon, Uber and Ebay, has led to increasing demand for cheap and secure payment solutions for low-value cross-border transactions.

[1] For example in 2021, cash accounted for 26% of POS transaction value, which was 15% lower than that of 2019.

Entry of new players and emergence of new value chains

The payments landscape has changed in recent years, with the entry into force of the PSD2 and developments in technology and FinTech introducing many new players and new payment solutions to the market.

Notably, the inclusion of TPPs brought Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs) into the scope of European payments market regulated by PSD2, alongside the traditional operators, such as banks and card networks.

Furthermore, a wider range of companies have become active in the market through e.g., third party licences, thus increasing competition. In almost all countries the number of licences for third-party providers has increased (more than 5% on average since 2014) though there are significant differences across Member States.

Alongside new entries, there has been a parallel process of market consolidation. In particular, some smaller payment providers, which were already operating in the market before the introduction of PSD2, struggled to adapt to the new rules and sold their businesses under this pressure.

Apart from market entry, recent years have also seen the emergence of new value chains as a result of novel cooperations between market operators. The growing presence and transaction value of e-wallets and e-money represent one of the key changes in the value chain of payments, together with increased competition on the payment markets as a result of the emergence of automated clearing houses schemes.

Prevalence of new technologies, obstacles to further development and longer term technological developments

New payment processes, such as contactless cards, and new means of payment, such as mobile wallets and instant payments, are accelerating the move from cash to cashless payments.

The most used contactless payment solutions, which have been integrated into almost all terminals in-stores in the EEA, are NFC-based, while other technologies such as QR codes, are gaining traction more slowly, especially in comparison with other parts of the world. The low uptake of QR code payments is mostly explained by the general satisfaction of European consumers with the multiple payment solutions and services that are generally fast, cheap, secure and convenient to use. At the same time, the European payments market is fragmented by multiple and often purely domestic actors.

Digital wallets (or e-wallets), which have become more prevalent as a result of the Covid-19 pandemic, are another disruptive innovation in the field of mobile payments powered by QR and NFC technologies.

Looking further into the future, open banking through open API frameworks is expected to become a global trend and transform the retail payment markets, while central banks' digital currencies, along with private sector cryptocurrencies, are predicted to have a big disruptive impact on the market over the next 20 years.

The review clause

Appropriateness and impact of the rules on charges

The rules on charges are appropriate and have mainly had a positive impact. There is no evidence of any previous assessment of the appropriateness and impact of the rules on charges by a national authority but the legal analysis in this study finds that the rules on charges are reasonable. Similarly, no negative effects or impacts have been evidenced, except in Italy, where the court concluded that the system of payments to the public administration provides that the payment commissions are in favour of the payment service provider and not

in favour of the beneficiary. The main conclusion from the evidence collected is that the impact of the rules on charges according to Article 62 was rather positive and that the rules are appropriate.

Limitations to the scope of application

The limitations to the scope of application set down in Article 2(3) and (4) of PSD2 have been transposed into national law in full (retaking the literal wording, including the exceptions) and they are applied across all Member States.

Access to payment systems

The provisions on access to payment systems in Article 35 of PSD2 as transposed into national law are deemed to be essential for the market entry of payment service providers, they have fostered market entry and supported the creation of a level playing field. At the same time, EBA has proposed to clarify further the reference to 'duly justified reasons' for refusing and terminating access to PIs/EMIs to accounts with credit institutions, and in particular to introduce criteria for refusing access to or terminating existing accounts. The EBA also proposed to provide further details on the notification process set out in Article 36 of PSD2 by requiring credit institutions to notify competent authorities within a specific timeframe for the reasons for refusing access to or for terminating existing accounts for payment and E-money institutions.

Appropriateness and impact of the thresholds for payment transactions

The exemption and the threshold under Article 3(l) of PSD2 are appropriate. The objective of this exemption is to ease the purchasing of tickets for an event or for transport through an electronic device as part of the provision of electronic communication services. The exemption and the threshold under Article 3(l) of PSD2 have been widely transposed into national law and there is no evidence that the threshold is unreasonable.

Possible introduction of maximum limits of amounts blocked on payer's payment account

Article 75 of PSD2 sufficiently balances the interests of PSPs and PSUs. Article 75 has been transposed into national law across all Member States and there is no evidence in relation to the necessity to complement this provision with maximum limits for the amounts to be blocked on the payer's payment account. The current amount and scope of Article 75 of PSD2 provides a sufficient balance of interests between the economic need for security of the account holding payment service provider to reserve a sum of money and the need for transparency for the payment service user.

Relevance

Relevance of PSD2 in light of market developments and policy priorities

The needs present at the inception of PSD2 largely continue to be relevant today. The only exception is the need to harmonise charging practices across Member States which has largely been achieved as a result of the surcharging ban. Indeed, the surcharging ban has harmonised charging and steering practices for a large share of payments in the EU. Where divergences exist, and a surcharge can still be charged, this concerns only a fraction of total payments. Also, in the rare case that they are charged, surcharges can no longer surpass the actual costs the merchant incurs for accepting the respective payment.

Continuing market developments, i.e. market developments that were present at the inception of PSD2 and continue to this day, affirm the relevance of a number of needs underpinning PSD2. For example, the need for more effective competition remains relevant in light of technical, commercial and regulatory barriers to entry, resulting in (continued) limited market penetration of innovative payment solutions and fragmentation of the European payments market. Other needs that remain relevant are the need for more harmonisation of licensing and

supervisory practices and increased consumer protection. Divergences in supervisory practices as well as developments in consumer fraud affirm the relevance of these needs.

New market developments similarly affirm the relevance of some of the needs that PSD2 aims to address, for example, the needs to regulate the status of all payment service providers and for more effective competition. These needs remain relevant as a result of the emergence of premium APIs and API aggregators. The new market developments also affect the needs for less fragmentation, as well as a more autonomous and resilient European payments market. The growth of domestic account-to-account payment schemes affects the first, whereas the entry of BigTechs to the European payments market affects the latter.

Finally, future policy developments have the potential to affect the needs surrounding the competitiveness, structure, autonomy and resilience of the European payment market. Most potential lies in the development of a pan-European payment solution and the adoption of instant payments. Were they to materialise successfully, they would increase competition and enhance consumer choice and innovation, reduce fragmentation, and enhance autonomy and resilience in and of the European payments market.

Expected future evolution of needs

Future developments in the payments market may impact the needs underpinning PSD2. For example, the introduction of a digital Euro, or the uptake of crypto-assets as a common form of payment, may increase competition and decrease fragmentation in and of the European retail payments market.

Other needs, such as for increased consumer protection or for a more autonomous and resilient European payments market, may similarly be affected. The uptake of crypto-assets as a payment method may affirm the relevance of increased consumer protection, as they are complex assets to understand. The adoption of a digital euro, i.e. a homegrown payment solution, would make the European payments market more autonomous and resilient (and thus reduce the relevance of that need).

Extent to which PSD2 addresses current developments in the field of payment services

The objectives of PSD2 continue to a large extent to address the current needs. The exception is the objective on steering charging practices across countries which has become less relevant, as it has to a large extent been achieved. Also, when a new need to strengthen the autonomy and resilience of the European payments market is introduced, accompanying objectives will have to be formulated.

Effectiveness

Overall, there has been progress in meeting the objectives of the PSD2, though issues in implementation have meant that these objectives have not been fully met, and market actors have faced some difficulties in operating in the new legislative environment.

The benefits of PSD2 so far have been significant and wide-ranging. These are as follows:

- Compared to previous legislation, the PSD2 has been a major step forward for the payments industry and it has brought about important benefits. For instance, it has allowed for greater competition, choice and innovation as new businesses and business models have emerged.
- Moreover, PSD2 provided the legislative and regulatory foundations for Open Banking, it has improved the security of payment transactions through the implementation of Strong Customer Authentication (SCA), allowed for a drop in fraud levels, and it has facilitated the adoption of electronic means of payments in the EU. SCA nonetheless is seen to have come at a significant cost.

- At the same time, the PSD2 has also increased consumer rights in various areas, such as reduced liability for unauthorised payments and unconditional refund rights for direct debits in euro.
- On the other hand, the study finds that the SCA requirement has made the customer journey in a transaction more difficult and cumbersome which can mean consumers do not complete e-commerce transactions. Moreover, there remain loopholes in SCA, which allow fraudsters to circumvent security provisions.
- PSD2 has contributed to a certain extent to developing cross-border payments within the EU and enhancing the quality of such payments, but the EU market remains fragmented along national lines and consumer awareness remains low. This is problematic because the share of fraudulent transactions is significantly higher for cross-border transactions than for domestic transactions.

When it comes to open banking, the PSD2 has allowed for structured interaction between ASPSPs and TPPs, but this has brought up some fundamental issues that need to be resolved. On the one hand, ASPSPs are concerned about the costs they incur due to the free access they are required to provide and the regulation-driven competitive disadvantage that this has created for them. On the other hand, TPPs argue that access is consistently hindered or of poor quality, thus affecting the quality of services they can provide.

The vast majority of consulted stakeholders thought that the implementation of the Directive was a cumbersome and lengthy process. The biggest obstacle for banks was regulatory uncertainty while TPPs reported issues regarding long licensing procedures and cross-border payment initiations due to technical challenges. Several provisions within the PSD2 have not been implemented in a harmonised way across Member States, which has created difficulties for entities seeking to provide services across borders.

There is agreement that oversight has increased as a result of the Directive, but there need for further improvements in supervision. Supervisors have not been able to address key issues raised by TPPs and ASPSPs effectively and efficiently, which in turn has hampered their ability to provide services in line with the expectations of PSD2.

Finally, the consulted stakeholders agreed that the PSD2 is well-intentioned, but that they have led to disproportionate requirements on PSPs when it comes to transparency requirements, licensing regimes, and SCA.

Efficiency

The costs associated with the implementation of PSD2 are significant and the largest cost items are:

- Open banking, and in particular API-development (estimated at €2.2 billion);
- SCA rollout, notably implementation costs (estimated at ~ €5 billion) and an increase in transaction failure rates (estimated at up to €33.5billion, though the real figure is likely to be lower); and
- Legal interpretation and uncertainty.

The main quantifiable benefits linked to PSD2 are:

- Improvement of the functioning of the Single Market (including increased market access for TPPs in the order of €1.6 billion);
- Unlocking the potential for innovation, especially when it comes to modernisation of IT infrastructure, open banking, the further development of consumer services (like financial planning tools); and
- More secure payment environment for customers and a reduction in fraud rates (worth ~ €0.9 billion per year), especially for more tech-savvy consumers

The overwhelming majority of banks and banking associations consulted for the study suggested that the costs of the PSD2 largely outweigh the benefits to them. National authorities and TPPs established before PSD2 was introduced were more positive about the general impact, but they tended to agree with the overall negative assessment.

At the same time, while the costs of the PSD2 were incurred in the initial stages (i.e. substantial investment costs), the benefits – though significant – are only materialising gradually, and it is therefore difficult to come to an overall conclusion regarding costs and benefits at this time. This is true both for market participants and for authorities, where the benefits seemed to be more visible in countries with less developed payment markets.

Opportunities for simplification and maximisation of benefits

Opportunities to simplify the level 1 legislation generally relate to the reduction of legal ambiguity, the large room left for interpretation by NCAs leading to inconsistent application. In addition, stakeholders would be in favour of a more technology-neutral legislation, a comment generally made for both APIs and SCA, which in their view would reduce burden. Specific aspects related to level 2 legislation, namely the '90-day rule' and technology neutrality were also identified.

Nonetheless, overall benefits of simplification are expected to be modest. At the same time, the results of the analysis of costs and benefits suggest that the most substantial items are sunk (one-off) costs that have already been incurred. Therefore, the potential for simplification is overall relatively modest, and with benefits only now becoming visible, it is too early for a comprehensive list of opportunities to maximise these benefits at this point.

Coherence

Overall, the PSD2 shows a fair degree of internal coherence but there is evidence of some incoherence when it comes to the level of implementation in Member States. Specifically, Article 2 (Scope), Article 3 (Exclusions) and Article 4 (Definitions) have been the object of clarifications by EBA following questions by market participants. Ambiguity in terms of PSD2's fundamental concepts and exemptions, and the subsequent heterogenous interpretation across the Member States bring about an uneven playing field, and they create an incentive for forum shopping.

Moreover, in the face of technological and market change, maintaining coherence with the overarching objective to facilitate the emergence of a well-functioning payment services market may require changes to the applicability of the PSD2 (e.g., to technical services providers).

The potential merger of the PSD2 and EMD2 legal frameworks is a challenging, but welcome opportunity to reduce overall complexity that would bring more clarity to EU payment legislation. The interplay between the requirements on access to payment systems under PSD2 and SFD should be addressed directly within the SFD review. In ensuring the coherence between the PSD and AMLD, it is considered crucial to follow and build upon the work conducted by EBA.

Concerning operational and security risks, the scope of PSD2 and DORA partly overlap. Article 95 PSD2 (management of operational and security risks) will in future be without prejudice to the full application of ICT risk management requirements laid out in Chapter II DORA. All operational or security payment-related incidents – previously reported pursuant to PSD2 – would be in future reported under DORA, irrespective of whether such incidents are ICT-related or not. To achieve consistency between new rules and current guidelines, the relevant ESA guidelines would need to be updated in the future to ensure their coherence with the new digital operational resilience framework.

Finally, with regards to the interplay between PSD and MiCA, clarification would be desirable in respect of the crypto-asset service provider (CASP) contracting with a payee to accept crypto-assets other than e-money tokens. In particular, it is asked whether such a CASP would

need to meet the same requirements on consumer, security and operational resilience as a regulated PSPN. Also, further clarification is recommended with regards to the treatment of safeguarded funds under MiCA and PSD2, as well as the definition of "funds" under PSD2.

EU added value

Overall, the PSD2 was and continues to be justified as it has been a major step forward for the development of retail payment markets in the EU, it has increased legal certainty and the security of payment transactions, strengthened supervision, and it has brought considerable EU added value in terms of contributing to a level playing field across the EU and aligning national rules when it comes to payment markets.

At the same time, the evaluation shows that there is room to further align rules across countries and reducing incentives for regulatory arbitrage, clarify obligations and limit margins for interpretation at national level, reduce implementation delays and fostering collaboration between supervisory authorities.

Based on the conclusions of the report, the recommendations are organised along three main pillars of improvement.

Pillar I: Recommendations on PSD2 scope and exclusions

Improve the consistent application of PSD2 across Member States and better align licensing and supervisory rules. The study has shown that one of the main obstacles to the PSD2 fulfilling its objectives relates to the way in which it is applied in the Member States. Different interpretations of the rules and delays in implementation lead to regulatory fragmentation across the Single Market, which creates the risk of forum shopping and regulatory arbitrage. To address this concern, the following two complementary **recommendations are proposed:**

1. **Setting up a standing committee for coordination with a schedule of meetings between EBA and the national authorities.** As part of this recommendation, the representative national supervisory authorities and EBA would form a standing committee with an annual schedule of meetings on PSD2 application issues. EBA and the national supervisory authorities would meet each other regularly and EBA would check national supervisory practices for PIs and EMIs, as well as the national application of PSD2 rules. EBA would regularly inform the Commission regarding schedule and outcomes; and
2. **Setting up a standing committee with a schedule of meetings among the central banks of the ESCB.** Under this recommendation, the representatives of national central banks of the eurozone and the ECB would form a standing committee with an annual schedule of meetings on PSD2 application issues.

Address competition issues. While PSD2 of course applies without prejudice to the application of competition law, including the Digital Markets Act (DMA), the report has shown that under the current PSD2 rules, Big Techs leverage network effects (due to their access to non-payments related data, existing customer base, technology), which could create market powers that may prevent or distort competition. In addition, there are different national approaches to the surcharging ban. To address these issues the following recommendations are proposed:

3. **Scheduling continued antitrust scrutiny to ensure effective competition investigations on overdraft conditions;**
4. **Regularly informing the European Parliament on the results of the investigations on Big Techs carried out at the national level;**
5. **Creating a public and distributed register with the results of the antitrust investigations;**
6. **Scheduling regular meetings between the ECB, NCBs and the network of antitrust authorities;**

7. **Addressing the operation of (retail) payment systems as a regulated business; and**
8. **Setting up an information structure (i.e. a list, ledger or map) on Member State choices on surcharging to establish which Member States used / did not use the option available within the PSD2.**

Address legal uncertainty about the scope of PSD2 and the applicable rules as a result of new value chains and payment processes created by new technological solutions. In the first instance, this will require working on the definitions within the PSD2 by building on the existing PSD2 text. This should start from a general definition of "payment service", which should describe the key features of a payment service compared with other financial services, as well as services ancillary to the execution of payments, which are not covered in the PSD2. Clarifying the definition of a payment service should reduce ambiguities and help with consistency in application in the face of new technological solutions that have fostered the rise of digital payments and are accelerating the move to cashless payments. To address this, the following recommendations are proposed:

1. **Inserting a residual normative clause in the PSD Annex on payment services;**
2. **The residual normative clause would have a broad scope that does not exclude any future PIS/AIS-like services and it would cover both funds and data associated with fund transfers/custody as well as monetary value memorised as e-money; and**
3. **Guidelines and coordination activity by EBA on the approach to the residual normative clause.**

Address legal uncertainty within the PSD2, which is a large cost item for market participants and leads to an uneven playing field. There is a need for a close interplay between PSD2, MICA and the future regulation of CBDCs, because of the impact that CBDCs and crypto-assets will have on cross-border payments and the competition between payment methods. At the same time, consumer protection needs might have to be rethought given these new methods of payments. To address these issues, the following recommendations are proposed:

1. **Establishing a legislative consolidation process between MICA and PSD2;**
2. **Revising the definition of funds in the PSD2 to cover e-money tokens;**
3. **Adding "quasi-fund" definition to cover asset-referenced tokens;**
4. **Inserting a chapter in the PSD2 title on PSPs covering authorisation and supervision of asset referenced token issuers and e-money token issuers;**
5. **Extending the application of the information requirements also to payment transactions by means of e-money tokens and asset-referenced tokens; and**
6. **Excluding the application of Title IV to payment transactions by e-money tokens and asset referenced tokens.**

Unify PSD2 and EMD2 to address legal uncertainty and diverging application of rules across countries and for different market participants. To address this a legislative consolidation between the two texts is proposed by:

1. **Adding a chapter on the authorisation and supervisory requirements for electronic money institutions in the PSD2 Title on PSPs;**
2. **Extending the application of Titles III and IV of the PSD2 to e-money payment transactions;**
3. **Removing preamble (6) of EMD2; and**
4. **Setting a single set of core definitions applicable both to e-money and payment services.**

Adopt more consistent definitions of the following main issues: access to accounts (within the PSD2+EMD2), access to payment systems (better within the FSD), agents/outsourcing (within the PSD2+EMD2). There are divergent approaches at national level to the "agent" exemption; divergent application practices for direct and indirect access of EMI and Pis to payment systems, which creates legal uncertainty, slows the development of

cross-border payments and represents a market barrier. To address this, the following recommendations are proposed:

1. **EBA guidelines on the "agent" exemption on a regular basis;**
2. **EBA guidelines on the indirect access of EMIs and PIs to payment systems; and**
3. **Consolidating the guidelines, PSD2 provisions and Q&As on "access to accounts" in the ASPSPs-TPPs relationship.**

Strengthen cooperation between national supervisory authorities over payment platforms and digital platforms providing payment services to prevent divergent application of PSD2 and divergent supervisory practices. This will reduce legal uncertainty about PSD2 rules and reduce costs for businesses. To address this, the following recommendations are proposed:

1. **Giving a legal framework to digital platforms providing payment services (for example: Amazon; Apple Pay, and so on) as foreseen in the DMA; and**
2. **Setting up a supervisory committee on platforms on a cross-border basis coordinated by EBA**.

Under this recommendation, the members of national supervisory authorities where the business platform operates join the committee chaired by EBA. They meet regularly and coordinate regulatory approaches and supervisory practices.

Pillar II: Recommendations on open banking

Address standardisation and interoperability issues, at least when it comes to QR codes, card-payment payment transactions, and API standards as these present a risk of legal fragmentation. To address these issues the following recommendations are proposed:

1. **In the eurozone, vesting the European Payment Council with a coordinating task; and**
2. **Establishing a SEPA-like incentive mechanism to make businesses cooperate on the regulatory and technical standards (i.e. Open Banking, QR codes, APIs and so on).**

Ensure that emerging payment service providers are covered by the regulatory framework governing retail payments in the EU to maintain the effectiveness of the PSD2 in the future. To address this, the following recommendations are proposed:

1. **Defining a three-tier "payment service" concept based on i) the transfer and custody of monetary assets (i.e., funds), as well as what is preliminary to send or receive funds, ii) the transfer and custody of data associated with the payment transactions, iii) the managing of payment platforms; and**
2. **Fostering closer cooperation among national authorities via EBA.**

Address FinTech industry concern that the implementation of PSD2 raises a range of obstacles and challenges that might affect the level playing field and effective competition. To address this, the following recommendation is proposed:

1. **Amending Article 97 of PSD2 to make it clear that once a payment service user authorises an AIS to access its payment accounts (through a mandate for instance), then that permission is valid on an ongoing basis until the user revokes access.**

Pillar III: Recommendations on data protection and consumer protection

Set a more efficient data authorisation and customer identity control system to reduce the PSD-based cost items linked to legal uncertainty. To address this, the following recommendation is proposed:

1. **Improving coordination between EBA and data protection authorities.**

Improve protection of payment service users in the context of growing cashless payment systems and the need to improve outcomes for users and trust in new payment methods. To address these issues the following recommendations are proposed:

1. **Setting different levels of protection and liability based on the user's degree of vulnerability (for example, elderly people);**
2. **Developing a cross-border ADR mechanism for cross-border disputes on rights and obligations for payment services;**
3. **Extending the existing data protection safeguards in the PSD2, information requirements and fund protection to all payment services, with no differences across legal forms of the PSP;**
4. **Considering the business entity providing licence-as-a-service liable for the custody/transfer of funds/data and for money laundering control because it facilitated the business activity of any ASPSPs using its licence; and**
5. **Streamlining the legal framework for information requirements by introducing one title in the PSD covering information duties for PIs, EMIs; issuers of asset-referenced and e-money tokens.**

1. Introduction

This document contains the Final Report for the Study on the Application and Impact of Directive (EU) 2015/2366 on Payment Services (PSD2).

1.1. Objective and scope of the study

The study contributes to the review of Directive (EU) 2015/2366 on Payment Services (PSD2) which entails a comprehensive assessment of the implementation and application of the PSD2. More specifically, the two main objectives of the study are to:

- Collect legal and economic evidence on the application and impact of PSD2 on the payment markets. The study also assesses benefits and challenges resulting from the Directive; and
- If areas of market failures, dysfunctioning or sub-optimal efficiency and effectiveness compared to the initial and current policy objectives are identified, advise on modifications of the PSD2 that can address them, in the context of a potential proposal for a revised PSD2.

In addition, the main requirements of the review clause (Article 108) are to assess:

- The appropriateness and the impact of the rules on charges as set out in Article 62(3), (4) and (5);
- 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;
- Access to payment systems, having regard in particular to the level of competition;
- The appropriateness and the impact of the thresholds for the payment transactions referred to in point (l) of Article 3;
- The appropriateness and the impact of the threshold for the exemption referred to in point (a) of Article 32(1);
- 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.

The study assesses whether the introduction of the PSD2 helped reach the five general objectives identified in the European Commission's impact assessment,2 namely to:

- Ensure a level playing field between incumbent and new providers of card, online and mobile payments;
- Increase the efficiency, transparency and choice of payment instruments for payment service users (consumers and merchants) (PSUs);
- Facilitate the provision of card, online and mobile payment services across borders within the EU by ensuring a Single Market for payments;
- Create an environment which helps innovative payment services to reach a broader market; and
- Ensure a high level of protection for PSUs across EU Member States.

The study also provides a set of recommendations on possible revisions of PSD2 provisions and clearly identifies their pros and cons. In doing so, the analysis differentiates between the

[2] European Commission (2013) Impact Assessment accompanying the document: Proposal for a directive of the European Parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC and Proposal for a Regulation of the European Parliament and of the Council on interchange fees for card-based payment transactions, pp. 35-36.

challenges which PSD2 already aims to address and new challenges, such as further/ongoing market developments, new market actors and whether those should be covered by the PSD.

The study will be used as a source of information for the Commission report required by the review clause in PSD2 (Article 108) and in the communication on a Retail Payments Strategy for the EU3, namely to:

- Take stock of the strong customer authentication's impact on the level of payment fraud in the EU and explore whether additional measures should be considered to address new types of fraud, in particular with regard to instant payments;
- Re-examine the existing legal limits on contactless card and wallet payments, with a view to striking a balance between convenience and fraud risks;
- Evaluate any new risks stemming from unregulated services, especially technical services ancillary to the provision of regulated payment or e-money services, and assess whether and how these risks can best be mitigated, including by subjecting the providers of ancillary services or outsourced entities to direct supervision. This could be done by bringing certain activities under the scope of PSD2 where justified;.
- Assess the adequacy of the exemptions listed in PSD2 and evaluate the need for changes in prudential, operational and consumer protection requirements;
- Take stock of the experience of new business models based on the access to and sharing of payment accounts data, with a view to informing a legislative proposal for a broader open finance framework; and
- Consider aligning the PSD2 and E-Money Directive (EMD2) frameworks by including the issuance of e-money as a payment service in PSD2.

[3] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Retail Payments Strategy for the EU (COM/2020/592 final).

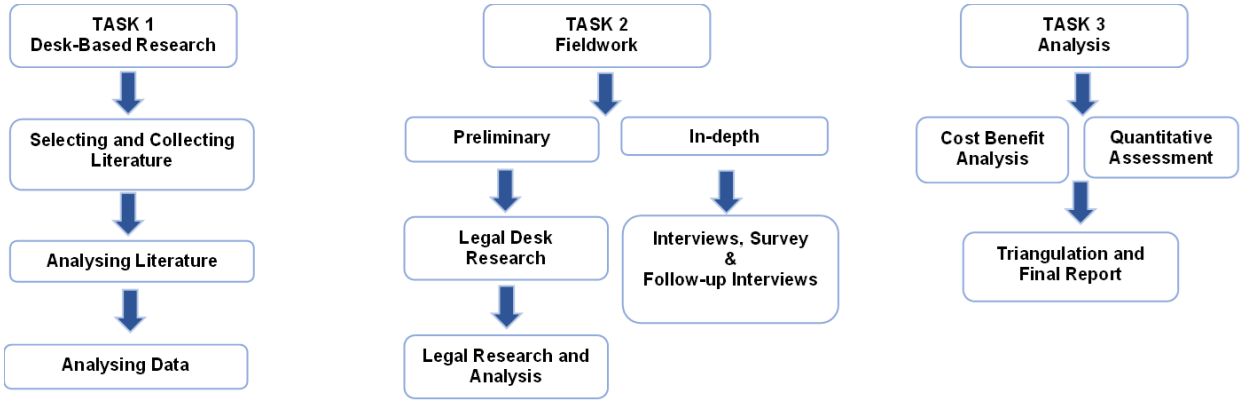
2. Methodological approach

This section presents the methodological approach to assess the application and impact of PSD2. The approach follows the Better Regulation Guidelines and Toolbox, as updated on 3 November 2021[4].

2.1. Methods and tools

The study comprises three tasks, namely: i) desk-based research (section 2.2); ii) fieldwork (section 2.3); and iii) analysis (section 2.4), as illustrated in the figure below:

Figure 1: Methodology process



The data collection activities are based on the conceptual understanding of the intended functioning of PSD2, in the form of an intervention logic (Annex 12). As noted in the Better Regulation Toolbox[5], intervention logics describe how an intervention was expected to work by identifying its main elements and linking activities with outputs and outcomes. They explain and identify the different actors and steps involved and depict cause and effect relationships.

In line with the recently released Better Regulation Toolbox, the intervention logic in this study builds largely on the problem tree of the impact assessment accompanying the original proposal for PSD2, taking into account the 'drivers' and 'problems' in the identification of needs, and the 'effects' for outputs and outcomes. The intervention logic was expanded to include all relevant items not specified in the problem tree, for instance regarding access to payment accounts rules.

The needs listed In the intervention logic link back to the main problems identified by the impact assessment before the introduction of PSD2, when PSD1 was already in force. Therefore, they link back to market failures (a fragmented market for innovative solutions and competition issues in some payment areas) and regulatory and supervisory gaps (the inconsistent application of PSD1 across Member States, legal vacuum for certain Payment Services Providers (PSPs), diverse charging practices and diverging supervisory and licensing rules and practices).

The Directive was guided by a hierarchy of five general and six specific objectives. The changes introduced by the legislation itself are 'inputs', namely: a) regulation and harmonisation of the status of TPPs; b) laying down access to payment accounts rules,

[4] Better regulation: guidelines and toolbox | European Commission (europa.eu). Particular focus has been made on the better regulation Toolbox on understanding the functions of PSD2 through an intervention logic and carrying out methodologies used for the cost-benefit analysis such as tools #56-58.
[5] European Commission (2021) Better Regulation Toolbox, p. 389.

including the lawful use of consumer data; c) prohibition of surcharges regarding specific payment methods; d) laying down a better claim resolution and reporting on security incidents; e) laying down requirements for SCA; and f) setting low ceilings for unauthorised transactions and laying down protection against theft or misappropriation of funds.

The four 'outputs' (improving the level playing field, lower payment fees, removal of barriers to cross border payments, improved customer protection and payment safety) summarise the key expected results following the introduction of the Directive. Finally, the 'outcomes' show the wider impacts on the payments market and the Internal Market. Besides market integration, innovation and a more consistent application of the rules, they also include reference to the broader goal of facilitating further uptake of non-cash payments.

Finally, the **evaluation matrix** (Annex 9) presents the logical link between the study objectives and the analysis. It operationalises the research questions to be considered in the assignment and connects them with judgement criteria and indicators. The evaluation framework furthermore links these, in a systematic and structured way, with the appropriate data sources.

2.2. Task 1: Desk-based research

Task 1 was dedicated to the review of the literature relevant to answering each of the evaluation questions. Desk research was based on different sources, including policy and academic texts, national and international datasets from both public and private stakeholders. The desk-based research fed into the answers to all evaluation questions and into the preparation of a survey, interview questionnaires and follow-up interviews. A list of consulted references can be found in Annex 4.

2.3. Task 2: Fieldwork

The aim of Task 2 was to collect all the necessary legal and primary evidence to respond to the evaluation questions. The fieldwork included the collection of questionnaires via surveys and interviews with a broad range of key stakeholders concerned with the application of the PSD2.

2.3.1. Legal research

National legal experts conducted legal desk research in 10 selected Member States, namely Belgium, France, Germany, Ireland, Italy, Lithuania, the Netherlands, Poland, Spain and Sweden. Annex 3 contains the research protocol that was used to collect data in each of the 10 Member States and Annex 5 contains a list of legal documents and law gazettes that were consulted in the research.

2.3.2. Primary data collection

The aim of the in-depth fieldwork was to gain a comprehensive picture of different views and perspectives on the study questions. It consisted of three components: i) interviews with relevant stakeholders in selected Member States; ii) a survey disseminated across the EU; and iii) follow-up interviews in selected Member States. The sample covered a wide range of actors which are impacted by the PSD2 to different extents, namely: i) payment services providers (e.g., banks, payment institutions); ii) payment services users (e.g., via consumer protection bodies); iii) national competent authorities (e.g., Ministries of Finance, Economics, Justice and Supervisory Authorities); iv) EU associations (e.g., banking associations, consumer associations); v) other actors involved in the payments market (e.g., merchants); vi) and other relevant stakeholders (e.g., national associations, such as associations representing persons with special needs). Annex 1 contains a stakeholder synopsis report which presents the results of the primary fieldwork. Annexes 6 and 7 include all the questionnaires used for interviews and survey.

2.4. Task 3: Analysis

The analysis includes three components: an analysis of potential costs and benefits following the revised Better Regulation Toolbox (BRT – mostly tools #56-58), a qualitative assessment to answer all the research questions and, finally, triangulation of the findings against different data sources and reporting.

2.4.1. Cost Benefit Analysis

Data for the cost-benefit analysis was collected as part of the data collection stages of Tasks 1 and 2. The different CBA steps and categories of different costs and benefits considered are described in detail in Annex 8.

Figure 2: CBA steps

2.4.2. Qualitative assessment of research questions

The cross-analysis of data was carried out by combining quantitative information collected through CBA with a qualitative assessment from interviews and desk research.

3. Overview of relevant payment market trends

This section provides an overview of the market that is regulated by the PSD2 including a description of trends since its entry into force, the main players that operate in the market and how this has changed, the kinds of value chains that have emerged and the importance of new technologies. The section sets the stage for the evaluation in Chapter 5 which looks in more detail at the relationship between the market and the PSD2.

More specifically, this section answers the following evaluation questions:

- What trends can be observed in the payments market since the implementation of PSD2?
- Since the entry into force of PSD2, which new players have entered and which players have left the market? Which of the new players are unregulated entities? Which type of payment services or businesses/ activities have emerged?
- What kind of value chains have emerged regarding cooperation among actors in the payments market?
- How widespread are new technologies used in the field of payments? Are there any potential obstacles to their further development? Which technological developments could be implemented in the long term?

The analysis builds upon the desk research, as well as a review of the relevant literature. It sets the stage for the review in Chapters 4 and 5. The main limitation of this section relates to the available data, which is not always comparable across countries and/or time, and the relative recency of the implementation of PSD2 which means that not all impacts can be picked up in published data yet.

3.1. What trends can be observed in the payments market since the implementation of PSD2?

In recent years, European retail payments markets have undergone a significant transformation including increasing availability of new digital contactless payments methods, and increasing usage of third-party payment initiation and account information aggregation services. The inclusion of TPPs brought Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs) into the scope of European payments market regulated by PSD2, alongside the traditional operators, such as banks and card networks:

- A PISP is a service to initiate a payment order at the request of a payment service user with respect to a payment account held at any bank in the European Union.[6]
- An AISP is an online service to provide consolidated information on one or more payment accounts held by a PSU with another PSP or multiple PSPs. The primary purpose of an AISP is to collect and provide information to the user including e.g., financial forecasting, money management, price comparison, personal finance and/or document management. AISPs depend upon Account Service Payment Service Providers (ASPSPs) and they cannot use customer data or log on to their payment accounts for any purpose other can those provided by the service.

The remainder of this chapter describes the main trends In the market for payment services in Europe that are relevant for the review of the PSD2, including point of sale, e-commerce and remote payments, cross-border payments and licensing trends.

[6] Donnelly,M, (2016), "Payments in the digital market: Evaluating the contribution of Payment Services Directive II", Computer Law & Security Review 32 (2016) 827–839

3.1.1. Point-of-sale (POS) market trends

Cash payments

Cash is still the most accepted payment method at POS. For example, according to the ECB, in 2019 almost three out of four in-store payments were made by consumers in cash. In some Member States, such as Austria, Germany, Italy and Malta, cash is still the most preferred and widely accepted method of payment at POS (Kantar Public, 2022).

However, since 2007, cash usage in POS retail payments has increasingly been replaced by cards and other electronic payment methods (Capgemini, 2010; EBA, 2019a; ECB, 2020; Kantar Public, 2022). In the same ECB study, only one in four consumers reported that they prefer paying in cash, while 49% answered that they would prefer a cashless means of payment, such as cards.

The pandemic has accelerated the trend towards cashless payments at POS. The shift in payment behaviour was mainly driven by consumer demand, because of the increasing preference to have less physical contact, and merchants' increasing offering of cashless payment solutions to protect their staff during the pandemic (Ecommerce Europe & EuroCommerce, 2021). According to ECB's SPACE survey (the study on the payment attitudes of consumers in the eurozone), 40% of the respondents in the eurozone stated that they have used less cash since the start of the pandemic, and a large majority stated that they would prefer continuing with cashless payments after the pandemic (ECB, 2020). In 2021, cash accounted for 26% of POS transaction value in the EU, 2 percentage points lower than in 2020 (28% of transactions value), and 15 percentage points lower than 2019 (41% of transaction value) (41% of transaction value) (Worldpay, 2022). Even in the most cash-intensive Member States, cash usage has experienced significant declines, such as in Germany, where cash usage accounted for 60% of total payments in 2020, down from 74% in 2017 (Bundesbank, 2021).

Beyond Covid-19, the main reasons behind the shift towards cards are greater security of funds, control over finances, and convenience, particularly due to increasing contactless payment options (ECB, 2020; Kantar Public, 2022).

Today, cash is increasingly used only for lower value day-to-day transactions or where it is the only accepted payment method (such as for some vending machines and tips). Since 2014, the number of payments made without cash has increased by more than a third and in 2020, the total number of non-cash payments in the eurozone, comprising all types of payment services, increased by 3.7% to 101.6 billion compared with the previous year and the total value increased by 8.7% to €167.3 trillion.

Table 1: Number of cashless payments in billion[7]

2014	2015	2016	2017	2018	2019	2020
68,3	73,5	77,9	83,8	90,7	98,0	101,6

Payment cards

Within cashless payments, the share of payment cards is continuously increasing at the expense of payments via credit transfers, cheques and direct debit cards. Today, payment cards are the most popular means of cashless payments at POS in almost all Member States, except for Germany and Bulgaria[8]. In July 2021, out of all cashless payments[9] made in Germany, only 29% were made with cards, the lowest of any Member State, and only 32% in

[7] Based on data from the ECB: https://sdw.ecb.europa.eu/reports.do?node=100000760
[8] With direct debits in Germany and credit transfers in Bulgaria being the most preferred cashless transaction method.
[9] Cashless payment methods include credit transfers, direct debits, card payments (except cards with e-money function), cheques, E-money payments, and other payment services.

Bulgaria, while in the EU card payments accounted for 50%[10] of all cashless transactions, with the highest share of card payments accounted in Denmark, Portugal and Romania at around 70% (ECB, 2021a).

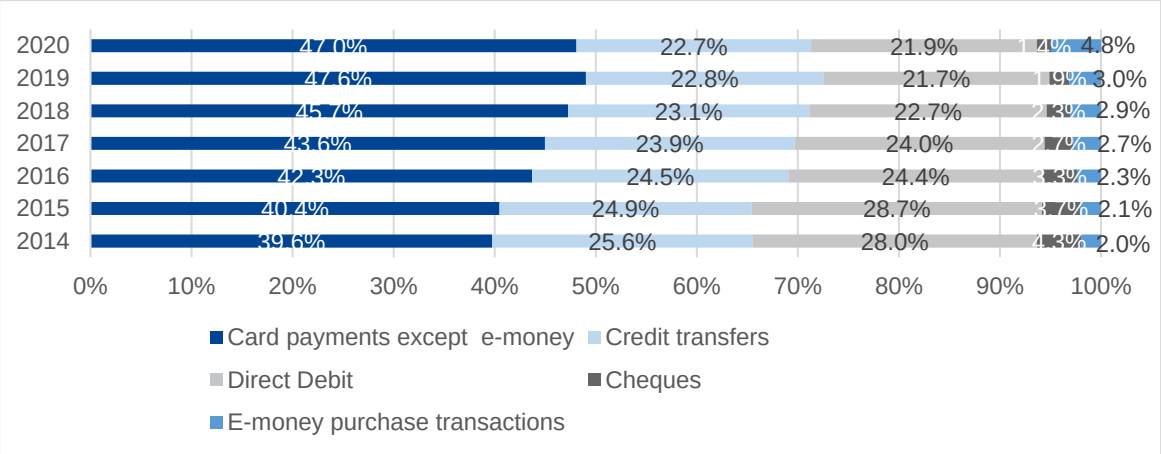
Debit and credit cards used to be preferred mainly for higher value transactions because of their perceived safety, record keeping and the possibility of delaying the settlement (for credit cards). However, the decreasing average card transaction value shows that card payments are increasingly replacing low value cash payments, with debit cards being the most preferred method of card payments (ECB, 2020; Worldpay, 2022).

Overall, the decreasing merchants' cost of accepting cards may have accelerated card usage at POS. Merchant'' cost of accepting card payments depends on merchant service charges (MSC) paid to the acquiring (merchant) bank and terminal fees for rental and/or maintenance of POS terminals. The merchant service charge is directly related to the interchange fee, which the acquiring bank pays to the issuing (customer) bank. Typically, interchange fees are passed on to the merchant as part of MSC. In 2015, the European legislator adopted the Interchange Fee Regulation (IFR), which capped the interchange fee for payments made with debit and credit cards. Interchange fees decreased in Member States following the introduction of the IFR, with the exception of Hungary where they remained the same (de Groen, 2020). Previous literature shows that lower interchange fees lead to lower merchant fees, which in turn can increase the merchants' card-based payment acceptance (Ardizzi & Zangrandi, 2018; Carbó Valverde et al., 2016). In 2019 and 2020 the number of POS terminals in the EU increased respectively by 8.3% and 5.1% (the highest increase in 2020 was observed in Luxembourg with 24.4%, followed by Czechia and Lithuania). Similarly, the number of payments at POS terminals in the EU increased by 10.4% in 2019 and only by 0.4% in 2020 due to a decrease in transactions during Covid-19 pandemic (ECB, 2021a).

E-money and digital wallets

POS payments through e-money are also increasing steadily, even if they are still at a low level.[11] These include e-money transactions by using e-money accounts (e.g., Paypal, ApplePay, among others) or online services that are based on bank transfers (e.g., iDEAL, SOFORT, among others).[12]

Figure 3: Cashless payment methods development[13]



[10] Including Luxembourg with 4.8% share of card payments, which exhibits a special case of very high number of e-money payments due to methodology applied, hence the relative importance of the payment instruments represented appears to be lower than their actual importance.

[11] https://www.ecb.europa.eu/press/pr/stats/paysec/html/ecb.pis2020~5d0ea9dfa5.en.html

[12] Payment choices in Europe in 2020. Payment_choices_in_Europe_in_2020__Convergence_at_.pdf

[13] Based on data from the ECB: https://sdw.ecb.europa.eu/reports.do?node=100000760

Indeed, electronic money, i.e. an electronic store of monetary value on a technical device that may be widely used for making payments to entities other than the e-money issuer[14] and digital wallets are key in the assessment of market trends and new technologies in the field of payments. Digital wallets are electronic payment tools that store payment cards or account details via a computer or smartphone to facilitate POS and online payment transactions. Digital wallets are mostly linked to one or more payment cards (or alternatively bank accounts) and built on the existing debit and credit card networks. Although digital wallets do not change how payments are processed, similar to traditional four-party card payment system, they do change the transmission of payment authorisation and format of payment authorisation data.

Consumers use digital wallets because there are no additional costs and they are convenient, since they may use biometric authentication instead of PIN codes, are contactless, and most consumers always carry their phone with them (Kantar Public, 2022; Oxera, 2020). In 2021, mobile wallets accounted for 7.7% of POS value spent in the EU, with Swedish customers adopting at the highest rate, 12.9% of POS transaction value (Worldpay, 2022).

Digital wallets can be broken down into different categories based on:

(i) Merchant acceptance (general-purpose or merchant-specific);
(ii) Flow of funds (staged or pass-through); and
(iii) Delivery technology they use (near filed communication, QR Codes, or digital/online-only) (Aite Group, 2016; Levitin, 2018).

Based on merchant acceptance, digital wallets can be differentiated as "merchant-specific" and "general-purpose" wallets. General-purpose wallets can be used for payments at any merchant (provided the merchant possesses a terminal with contactless payment technology at POS or offer online sales), such as Apple Pay, Google Pay, Samsung Pay, and Paypal, whereas merchant-specific wallets, like Starbucks App and Amazon Pay (incl. Amazon 1-Click), can be used only with the specific merchant that issued the wallet to purchase their goods and services.

Digital wallets can also be classified based on the flow of the funds as "staged" and "pass-through" wallets. Staged wallets, such as PayPal and Lydia, divide the payment into two different stages in order to complete the transaction: funding stage and payment stage. In the funding stage, the customer makes funds available to the digital wallet. In the payment stage, the wallet moves the funds to the merchant. On the other hand, pass-through digital wallets act as a proxy for physical payment cards for instance, such as Apple Pay and Samsung Pay, and pass the customer's payment credentials to the merchant, which has the transaction processed directly by the acquirer bank. Therefore, the pass-through wallet is not involved in the movement of funds and funds are not stored by the wallet operator.

Finally, digital wallets can be classified based on their delivery technology. Many digital wallets use near-field communication (NFC – see also section 3.4) chips to communicate with (closely) located card/smartphone reading terminals, for instance Samsung Pay. Some other digital wallets use QR codes (Quick Read – see also section 3.4) that contain information which enables a customer or a merchant to initiate a payment transaction, such as Starbucks App. Digital/online-only wallets, such as PayPal and Amazon Pay, are designed for online usage (e-commerce and peer to peer transactions) only and have limited application at POS.

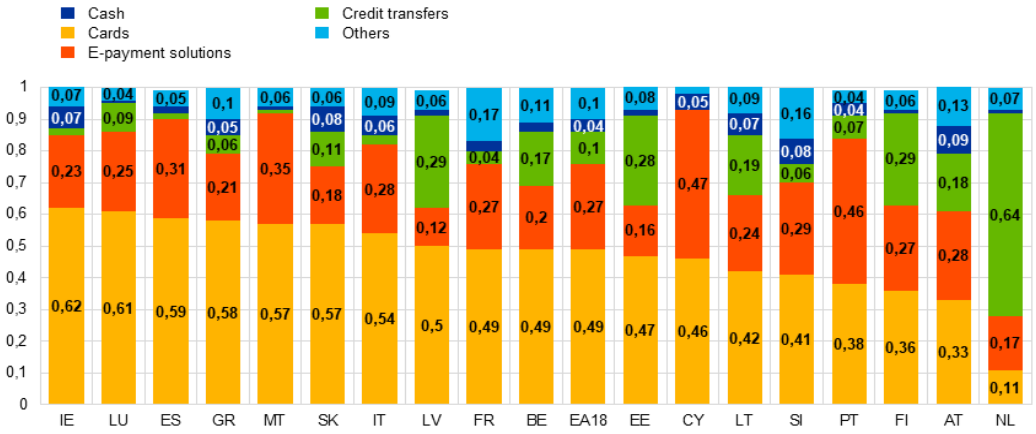
[14] https://www.ecb.europa.eu/stats/money_credit_banking/electronic_money/html/index.en.html

3.1.2. E-commerce and remote payments market trends

In 2020, Covid-19 lockdown measures and other restrictions accelerated the surge in e-commerce. According to Eurostat (2021), e-commerce, which includes sales via own websites and online marketplaces, accounted for 20% of the EU's total retail turnover in 2020. Among the Member States, the percentage of merchants making online-sales ranges from 40% in Ireland with, followed by Denmark (38 %), Lithuania and Sweden (both 36%) to 12% in Bulgaria and Luxembourg. Most of the merchants only offer online sales to customers in their own country (8% of merchants in 2020) (EC, 2019).

There is significant cross-country variation in payment instruments used in e-commerce. The figure below shows the share of different payment instruments in online purchases by country in 2019.

Figure 4 Online purchases per payment instrument and country



Source ECB (2019)

The most frequent payment method in e-commerce are payment cards. In 2021, card payments were the most preferred method of payment in e-commerce, where credit cards account for 25% and debit cards account for 17% of total e-commerce transaction value in the EU (Worldpay, 2022). At national level, in Belgium, Denmark, France and Ireland, card payments accounted for half of e-commerce transaction value in 2021, whereas online bank transfers were the most popular payment method for e-commerce transactions in the Netherlands (60% of transactions value), Poland (54% of transactions value), and Finland (31% of transactions value). In Germany, Spain and Sweden customers relied mostly on digital wallets (primarily PayPal in Germany, BBVA Wallet in Spain, and Swish in Sweden). By 2021, digital wallets and BNPL schemes accounted almost half of the e-commerce transactions value in these countries.

Online bank transfers currently represent the preferred alternative to card-based online payments for e-commerce (Ehrentraud et al., 2021). The service can be provided directly by banks or by third party payment initiation service providers (PISPs), which can facilitate a direct transfer of funds from the customer's bank account to the merchant's bank account.

Buy-Now-Pay-Later (BNPL) schemes are the third most popular payment option behind card and account-based payment methods in e-commerce (Worldpay, 2022)**.** BNPL is a financing arrangement through which a customer can spread out the total cost of a purchase over instalments. It is similar to delayed payments with credit cards. However, the main difference is that BNPL doesn't charge any interest or fees. When shopping online, customers who opt for BNPL make a small down payment (usually 25% of purchase price) and pay the remaining amount in a series of interest-free instalments, whereas merchants receive the full purchasing amount minus the fees paid to BNPL provider immediately. Although there is no risk of non-payment for merchants, BNPL service fees are higher than card processing fees,

which reduces the attractiveness of the service for small merchants. As of 2021, BNPL accounts for only 2% of the total e-commerce transaction value in the EU, but with increasing e-commerce activity, the share of BNPL, particularly for large merchants, is expected to increase in the next five years (Worldpay, 2022). BNPL is particularly strong in the German and Nordic retail payment markets. In Sweden, BNPL accounted for 25% of the e-commerce transaction value in 2021, in Germany for 20%, in Finland for 13% and in Denmark for 12% of the e-commerce transaction value. The BNPL market in these countries is primarily dominated by players from FinTech industry such as AfterPay, Klarna, Clearpay, Scalapay, Sezzle and PayPal. European banks have none to very limited BNPL offerings; the majority of European banks offer delayed payments with credit cards instead of BNPL services (Howell & Krulišová, 2021).

Finally, the use of e-invoicing is also expected to increase with increasing digitalisation and open API infrastructures. E-invoicing is a digital invoicing tool that enables consumers to pay after delivery without sharing their credit card or bank details. This solution can still be card-based to the extent that the subsequent payment of the e-invoice is linked to a payment card. The most important players that offer e-invoicing in the EU are Klarna and Afterpay.

3.1.3. Cross-border payments trends within the EU

Although a well-functioning cross-border payment infrastructure plays a crucial role for the integration of the EU economy, cross-border payments have often been slow, inefficient, and costly for banks and merchants. In the last decade, rising e-commerce activity and digital payments have increased demand for secure and cost-effective cross-border payment systems within the EU (PwC, 2021). However, existing domestic retail payment infrastructures are not designed for handling cross-border payments; the payments are not instant; the costs and compliance risks following from anti-money laundering and countering the financing of (AML/CFT) programmes tend to be higher, and small payments (for example, remittances) are penalised due to high fees. (Landau & Brunnermeier, 2022).

Major efforts have been made to accelerate cross-border payments within the EU, such as the introduction of single euro payment area (SEPA) standards for euro transactions, or the cross-border payment regulation (Regulation (EU) 2021/1230EC No 924/2009), which equalised fees for cross-border and national payments in euros, and finally to some extent PSD1 but mainly PSD2, which has the objective to accelerate the cross-border payment activity by:

- Introducing an EU passport procedure for PSPs to operate in multiple Member States;
- Allowing the entry of non-bank providers; and
- By increasing the transparency of fees applied to cross-border transactions.

The rise of online market platforms, such as Amazon, Uber and Ebay, has led to increasing demand for cheap and secure solutions for low-value cross-border transactions (Swift, 2018)(Swift, 2018). The entry of non-bank players into the payment markets allowed the development of new digital payment solutions, such as digital wallets with cross-border application, which can facilitate cross-border payments by allowing consumers to operate in multiple currencies.

3.1.4. PSD2-licensing trends

Licences for third-party providers (TPPs) have increased in almost all EU countries. Between 2014 and 2020, the number of licences issued across the EU increased by 190.

The distribution of third-party licences across countries has always been uneven. One possible reason for this is that some Member States may be reluctant to supervise e-money institutions due to their complex business models and the lack of skilled staff.[15]

Since PSD2 the differences between countries have accentuated. In 2014, there were comparatively many licences on the Swedish and Italian markets in 2014. Between 2014 and 2020, the distribution has changed. With 90 licences, almost half of the increase in licences since 2014 are attributable to Lithuania. In 2020, there are almost six times more licences registered in Lithuania in comparison to Sweden.

Table 2: Number of PSD2-licensed third-party providers 2014 and 2020[16]

	BE	DE	ES	FR	IT	LT	NL	PL	RO	SE	EU[17]
2014	29	53	75	44	73	40	36	33	14	97	882
2020	32	90	81	38	53	130	37	44	15	100	1072

One reason for this could be the simplified licensing procedure in Lithuania. According to stakeholders consulted for this study, the approval process in Lithuania is usually much shorter than in all other countries. One source indicated that the average timeline for an e-money institution to obtain a licence is between 4 to 8 months from the date of application.[18] Furthermore, Lithuania offers a special visa programme to the founders of start-ups, whereby they acquire a residence permit as part of the licensing procedure.

Brexit has also led to an accentuation of differences in the number of licences per country. Indeed, many TTPs domiciled in the UK chose to obtain an EU licence in Lithuania. In 2021, the Bank of Lithuania examined about 100 licensing applications and 20 out of all the EMIs and PIs now operating in Lithuania are UK capital entities.[19] Similarly, many start-ups have considered Germany as a base from which to obtain European passporting rights to provide payment services across the EU. [20]

In contrast, there is significantly slower growth or even a decline in licences in some other markets, such as in France. Possible reasons for this decrease may be that electronic money distributors are not registered by the French supervisory body (ACPR) [21] and thus do not appear in the public register of financial agents. It is common in the French payment market that some licensed players offer gateways that allow payment services that are not licensed to function under the guise of their licence. This has allowed unlicensed institutions to function within the French market without having the need to go over the licensing process and bearing the cost of obtaining a licence, as well as the costs of the associated supervisory framework. Finally, the French payments market has been experiencing a withdrawal of licences due to the lack of safeguarding of customer funds. [22]

There are also big differences between countries in the relevance of PSPs for the national payment market. Across the EU, the share of third-party providers has increased by more than 5% since 2014. However, in large economies, the share of PSP seems to be rather low, with the exception of Spain. In Sweden, the share of PSP was already three times higher than the EU average before PSD2. This could also be due to the strong integration of the Nordic banking market, which reduces the total number of registered payment service providers. For example, the largest bank in the Swedish market is registered in Finland. Over

15 E-money Licence Lithuania (Electronic Money Institution/EMI) - PSP Lab
16 Based on ECB data: www.ecb.europa.eu/stats/financial_corporations/list_of_financial_institutions/html/index.en.html
17 It should be noted that the data in the table for both years do not include any figures on the UK.
18 Lithuanian EMI Licensing Electronic Money Institution | 7 Need To Know New Points (tba-associates.com)
19 Lithuanian E-Money Transactions Skyrocket in 2020 - FinTech in Baltic (fintechbaltic.com)
20 Applying for a Payment Service Licence in Germany | Perspectives | Reed Smith LLP
21 Autorité de Contrôle Prudentiel et de Résolution
22 New Payment Stakeholders Overview | Banque de France (banque-france.fr)

time, the share of PSP has increased in all countries except Romania even though the increase in France and Italy is not very significant.

Table 3: Licensed PSPs as a share of overall payment institutions[23]

	2014	2015	2016	2017	2018	2019	2020
Belgium	22,31%	22,66%	29,13%	19,23%	19,61%	25,49%	28,83%
Germany	2,85%	2,85%	3,08%	3,44%	3,78%	5,04%	5,71%
Spain	25,00%	24,13%	27,62%	25,90%	26,49%	28,99%	29,67%
France	13,13%	13,41%	13,42%	13,67%	14,14%	14,49%	13,82%
Italy	10,00%	10,35%	11,13%	7,36%	7,97%	9,46%	10,06%
Lithuania	31,01%	34,56%	37,59%	46,10%	53,89%	59,49%	62,50%
Netherlands	14,63%	15,29%	29,23%	28,57%	29,51%	27,69%	30,33%
Poland	4,67%	5,66%	6,03%	6,47%	6,55%	6,88%	6,69%
Romania	26,42%	30,77%	30,19%	32,00%	31,25%	33,33%	17,86%
Sweden	38,65%	39,61%	40,70%	42,80%	43,23%	44,73%	39,84%
EU[24]	12,04%	13,08%	14,75%	15,90%	16,51%	17,33%	17,53%

The increase over time is strongest in Lithuania and the Netherlands, where the share has more than doubled. A clear increase can also be observed in Poland and Germany, albeit at a lower level which can be due to the importance of local players in these two countries. In Lithuania, the share of third-party providers was three times higher than the EU average in 2020 while it was three times lower than the EU average in Germany. In contrast, Sweden and France experience a minor decrease in the share of licensed third-party providers on overall payment institutions, while Romania alone suffered a significant fall in its share of licensing.

Finally, the table below shows the number of payment services providers in the EBA and ECB register of payment and electronic money institutions under PSD2 as of January 2022.[25] The countries with the highest number of credit institutions were Germany, followed by Austria and Italy. The country with the highest number of electronic money institutions in 2022 was Lithuania with 87. Exempted payment institutions are particularly prevalent in Poland (288) because the country offers a waiver to small PIs in contrast to countries like Spain or Germany which have stricter rules for market entrants (see also Chapter 4 on the review clause).

Table 4:Overview of payment and electronic money institutions under PSD2 in the EU27 based on EBA and ECB registries

Country	Credit institutions	Exempted electronic money institutions	Electronic money institutions	Institutions entitled to provide payment services	Exempted payment institutions	Service providers excluded from the scope of PSD2	Payment institutions	Account information service providers	Grand total
AT	460					55	7		522
BE	67	2	7		1	3	32	4	509
BG	22		8			13	11		492
CY	14		15				11		486
CZ	41	20	3		117	11	28	3	642
DE	1398		11			945	75		1491
DK	71	6	4		22	36	19	8	555

[23] Calculated by VVA based on data from the ECB: https://sdw.ecb.europa.eu/reports.do?node=100000760
[24] It should be noted that the data in the table for both years do not include any figures on the UK.
[25] https://www.eba.europa.eu/risk-analysis-and-data/register-payment-electronic-money-institutions-under-PSD2

Country	Credit institutions	Exempted electronic money institutions	Electronic money institutions	Institutions entitled to provide payment services	Exempted payment institutions	Service providers excluded from the scope of PSD2	Payment institutions	Account information service providers	Grand total
EE	10		2		5		18	1	486
ES	9		9		9		61	1	540
FI	23	6	2	2	41		18	10	539
FR	10		17			83	73	8	641
GR	42		3			2	10	1	476
HR	10	1	4	1		14	4	2	486
HU	13		2			1	10	6	479
IE	12		17	288		22	22	4	813
IT	403		11		1	104	51	4	631
LT	7	8	87		14	1	49	4	623
LU	176		10			2	15		487
LV	8	10	4	9	8	2	6		499
MT	18		26				24		510
NL	18	20	11		61	49	73		674
PL	17		1	35	1940		49	11	2496
PT	13		1				13		474
RO	13		2			7	10		479
SE	122	1	6		50	23	56	15	611
SI	12		3			9	2	2	476
SK	21		1		4	20	11	1	497
Grand Total	**3030**	**74**	**267**	**335**	**2273**	**1402**	**758**	**85**	**5654**

Source: EBA register, as of January 2022

3.2. Since the entry into force of PSD2, which new players have entered and which players have left the market? Which of the new players are unregulated entities? Which type of payment services or businesses/ activities have emerged?

3.2.1. Entry and exit of market players

As mentioned in the previous section, the rise in digital payments and access to payment accounts requirements led to the entry of new players in European retail payment markets including FinTechs and Big Techs (or TechFins). FinTechs are technology providing financial services start-ups, that are formed at the intersection of financial services and technology (Camerinelli, 2017). On the other hand, BigTechs/TechFins are technology companies, with established presence in the market for digital services (such as ecommerce, social media, payments, etc.) (Frost et al., 2019).

The adoption of PSD2 in November 2015 caused a rapid but temporary surge in the number of FinTech start-ups in Europe. After the transposition of the Directive in 2018 the number of new entrants fell and by the end of 2019 almost 75% of all PSD2 licences were granted to entities that were established before PSD2, with only a fourth of new licences given to new FinTech startups (Polasik et al., 2020).

BigTechs, such as, Google Pay, Amazon Pay and payments on Facebook Messenger, operate as payment and e-money institutions in the EU. The financial services that BigTechs offer, has especially been growing in lending to small and medium-sized firms (SMEs).[26] The table below provides an overview of BigTechs with a payment licence in Europe. From 2018 there was a significant increase of licensed BigTechs in the EU payments market, with the majority choosing an E-money Licence. This is because, licensed e-money institutions are allowed to issue e-money and they can store client funds for a long time period. In addition, under PSD2, licensed payment institutions (such as e-money) can passport their services to other EU countries, enabling licensed BigTechs to explore business opportunities in other EU countries.

Table 5 BigTech Payment Licence in Europe

BigTech Firm	Year of Licence	Type of Licence	EEA National Competent Authority
PayPal	2007	Banking Licence	CSSF- Luxembourg
Amazon Payments Europe	2010	E-money Licence	CSSF- Luxembourg
eBay	2014	Payment Institutions Licence	CSSF- Luxembourg
Rakuten Europe Bank	2016	Banking Licence	CSSF- Luxembourg
Facebook Payment Intl Ltd	2018	Payment Institutions Licence	Central Bank of Ireland
Alipay Limited	2018	E-money Licence	CSSF- Luxembourg
Airbnb Payment	2018	E-money Licence	FCA-UK
Google Payment Lithuania	2018	E-money Licence	Lietuvos Banka-Lithuania
Google Payment Ireland	2019	E-money Licence	Central Bank of Ireland
Uber Payment	2019	E-money Licence	De Nederlandsche Bank-Netherlands
Takeaway.com	2019	Payment Institutions	De Nederlandsche Bank-Netherlands
Zalando Payment Solution	2019	E-money	BaFin – Germany

Source: Compact (2020) [27]

Another development that has led to new players entering the market, even if indirectly, is licence-as-a-service. Companies that have a PSD2 licence and have established API connections to a large number of ASPSPs are effectively offering the use of this licence.[28] For instance, companies whose business revolves around the account information or payment initiation of their customers would facilitate a payment based on exactly the same account information or initiation payments as they would via a PSD2 licence, without needing a licence. In practice, they would use another provider's licence to obtain the information or trigger the payment for which their customer gives consent.

The typical three-party scheme, leaves room for fourth parties, i.e. all those players who do not have financial services as their core business, but want to take advantage of the

[26] EBA BoS 2019 (Thematic report on the impact of FinTech on PIs' and EMIs' business models).docx (europa.eu)
[27] Will BigTechs change the European payments market forever? - Compact
[28] The ACPR provides an overview of new payment players | Banque de France (banque-france.fr)

opportunities offered by open banking. The PISP licence, in particular, allows to initiate the transfer of money from a current account by SEPA credit transfer,[29] while the company does not have to apply for its own licence. For example, there are providers that advertise the use of a licence granted by the German BAFIN. In a similar context, in France licensed players offer technical gateways that allow unlicensed companies to offer payment solutions under the guise of the licensed players (see also Section 3.1.4 on licensing trends). [30]

The question naturally arises as to whether security is still assured in this way, since secure communication is explicitly required by the PSD2. Furthermore, this could have a significant impact on assessing the emergence and exit of new market players. In the long run, fewer market participants would need to obtain their own licences and a few PSD2 licences could be used by a large number of companies. This could weaken competition and make supervisory oversight more complicated, as supervisors would have less direct contact with most payment service providers. At the same time, it should be pointed out that the ACPR saw other possible risks from such a licencing model as more significant,[31] including management of Money Laundering and Financing of Terrorism (ML-FT) by the licenced player.

While there has been market entry as described above, this has gone alongside a trend towards consolidation in the market, as demonstrated by the takeover of SOFORT by Klarna, for example. More specifically, such consolidations within the payment services market, may affect the level of competition especially for banks, as they may lose clients from parts of their Tier 1 and Tier 2. [32]

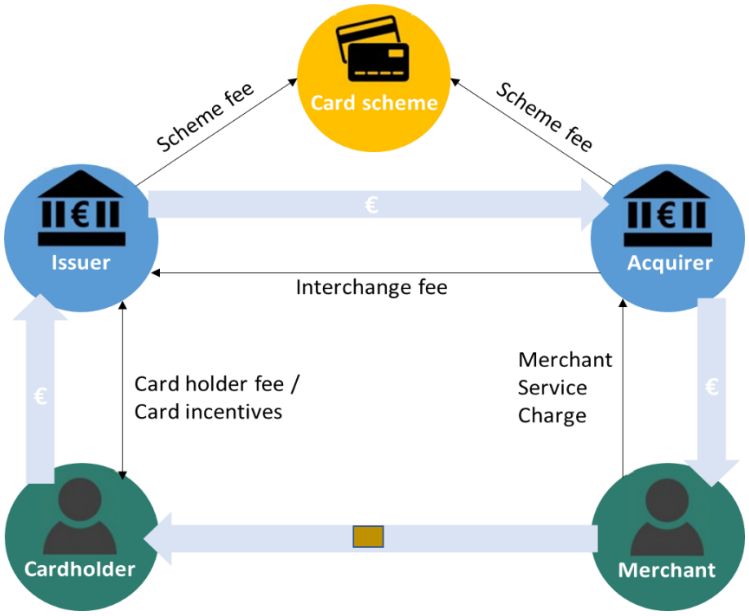
3.2.2. Type of payment services or businesses/activities that have emerged

As already indicated in the previous sections, the payments market is characterised by a wide range of market players with different entry points, offerings and competitive advantages. Some new market players entered the payment market without an existing customer base to offer services that draw their attraction from the simplicity of the payment for the customer. Older market participants include banks that have been using their existing customer base and existing interbank-processing infrastructure to enable payments online. A third group includes large retail companies which have used their existing customer base and introduced new payment methods.[33]

Currently, two international card schemes Mastercard (Maestro, Debit Mastercard) and Visa (V Pay, Visa Debit), are the major players in the EU market for card payments. Most debit and credit card payments in the EU are four-party payment schemes, which consist of a payer (customer, cardholder), a payer's PSP ("issuer bank"), a payee (merchant) and a payee's PSP ("acquirer bank"). The fifth party involved in the process is the card scheme, which facilitates the communication between the issuer bank and acquirer bank.

29 https://www.fabrick.com/wp-content/uploads/2021/09/210927_1326_FABRICK_PISP.pdf
30 The ACPR provides an overview of new payment players | Banque de France (banque-france.fr)
31 Ibid.
32 https://www.oliverwyman.com/our-expertise/insights/2018/dec/european-consolidation-in-payments.html
33 https://truelayer.com/blog/psd2-4-years-on-why-open-banking-is-a-success-and-how-to-judge-it

Figure 5: Traditional four-party card scheme



Source: De Groen (2020) based on European Commission (2016).[34]

Before the IFR, banks in some Member States[35] **decided to replace domestic card schemes with international schemes**, and in Member States where a domestic card scheme is present the majority of cards are co-branded with an international card scheme for cross-border payment acceptance. The domestic card schemes in the EU are Bancontact in Belgium, Borica/BCARD in Bulgaria, Dankort in Denmark, Carte Bancaire in France, Girocard in Germany, PagoBancomat in Italy, Multibanco in Portugal, Activa/Karanta in Slovenia, and STMP in Spain. Currently in the EU, only international card schemes are active for cross-border transactions (EY & Copenhagen Economics, 2020)(EY & Copenhagen Economics, 2020(EY & Copenhagen Economics, 2020).

Although PSD2 opens the EU payment market to competition, it may also set the stage for potential partnerships between traditional PSPs and TPPs. Banks and FinTech companies may decide to partner with banks providing the banking services and infrastructure and FinTechs delivering the consumer experience. This partnership works by banks opening up their services to FinTech companies through APIs (Camerinelli, 2017). Notably, few banks perceive FinTechs as a competitive threat, in part as a result of their limited scale and potential to reach customers (Maus & Mannberg, 2019). This is especially true in a country like Spain, where the major banks already have a very advanced digital offering (Rolfe et al., 2021). Instead, the majority of banks view FinTechs as potential partners who can spur innovation and help them achieve faster time-to-market (Borgogno & Colangelo, 2021). According to Tink (2020), 69.8% of banks (that did not already partner with a FinTech) prioritised establishing a FinTech partnership to access open banking technologies within the following 12 months.

3.2.3. Unregulated new market players

The Open Banking environment also fosters potential partnerships between regulated and unregulated entities. Technical service providers (TSPs) are unregulated players in the PSD2 ecosystem, which provide services on behalf of regulated entities, such as IT maintenance services, SCA authentication services, or unified API gateways and hubs. TSPs can operate on both the demand and supply side of the open banking environment. On the

[34] European Commission (2016), "Antitrust: Regulation on Interchange Fees", MEMO/16/2162
[35] For example, in Ireland and the Netherlands.

supply side, TSPs provide technical services to an ASPSP by hosting APIs on their behalf, and on the demand side, TSPs can provide technical services to AISPs and PISPs to access APIs.

In addition to technology providers, some regulated PSPs also operate as TSPs for other regulated PSPs (EBA, 2018a; Reynolds & Johnson, 2021). For example, a Mobile Initiated SEPA (Instant) Credit Transfers (or MSCT) service provider could be a PSP (e.g., an ASPSP or any party acting as a PISP under PSD2) or a technical service provider supporting a PSP (EPC, 2022).[36] Use of a TSP can have cost saving effects for the regulated entities, since it reduces the development efforts and operational costs due to economies of scale.

As the payment ecosystem expands to accommodate broader services, there is an expectation that these additional services will also be implemented using APIs, which can also create new risks in terms of unregulated services (EBA, 2018a; Farrow, 2020; Reynolds & Johnson, 2021). In terms of TSPs, one risk cited in the literature is the spill-over effect of unregulated entities over regulated entities. For instance, if a TSP faces operational and/or financial issues, this could lead to spill-over effects on regulated PSPs in terms of freezing of services.

Such issues highlight the importance of outsourcing agreements between PSPs and TSPSs. However, literature underlines that regulations concerning outsourcing agreements are not harmonised across Member States, and overlooked by national supervision authorities (Grabowski, 2021).

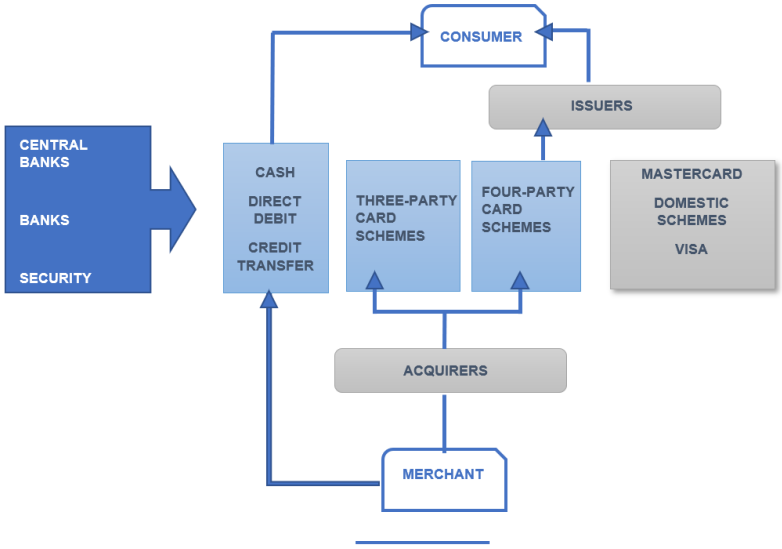
3.3. What kind of value chains have emerged regarding partnerships between actors in the payments market (e.g., between PSD2 supervised actors and non-supervised players)?

Value chains in the payments market have undergone a significant evolution over the last decade.[37] Notably, the inclusion of new services (Third-Party Payment Service Providers, namely PISPs and AISPs as described in the previous sections) under PSD2 spurred new opportunities for businesses and consumers.[38]

This extended (compared to PSD) definition of payment services reconfigures the value chain by reducing the need for active bank participation in a payments service. In fact, by getting direct access to a customer's account, third-party providers are able to build services on top of a bank's existing data and infrastructure[39]. Disintermediation of the banking value chain is the main driver of the open banking phenomenon. Figure 5 below displays some of the key actors which, together with providers of technical solutions/devices (e.g., credit cards and merchants' terminals manufacturers) make up traditional payment value chains for cash and card transactions.

[36] EPC024-22v0.6 Standardisation of QR-codes for MSCTs.pdf (europeanpaymentscouncil.eu)
[37] Oxera (2020), The competitive landscape for payments: a European perspective
[38] https://www.europeanpaymentscouncil.eu/sites/default/files/infographic/2018-04/EPC_Infographic_PSD2_April%202018.pdf
[39] Oxera (2020), The competitive landscape for payments: a European perspective

Figure 6: Traditional payment value chain



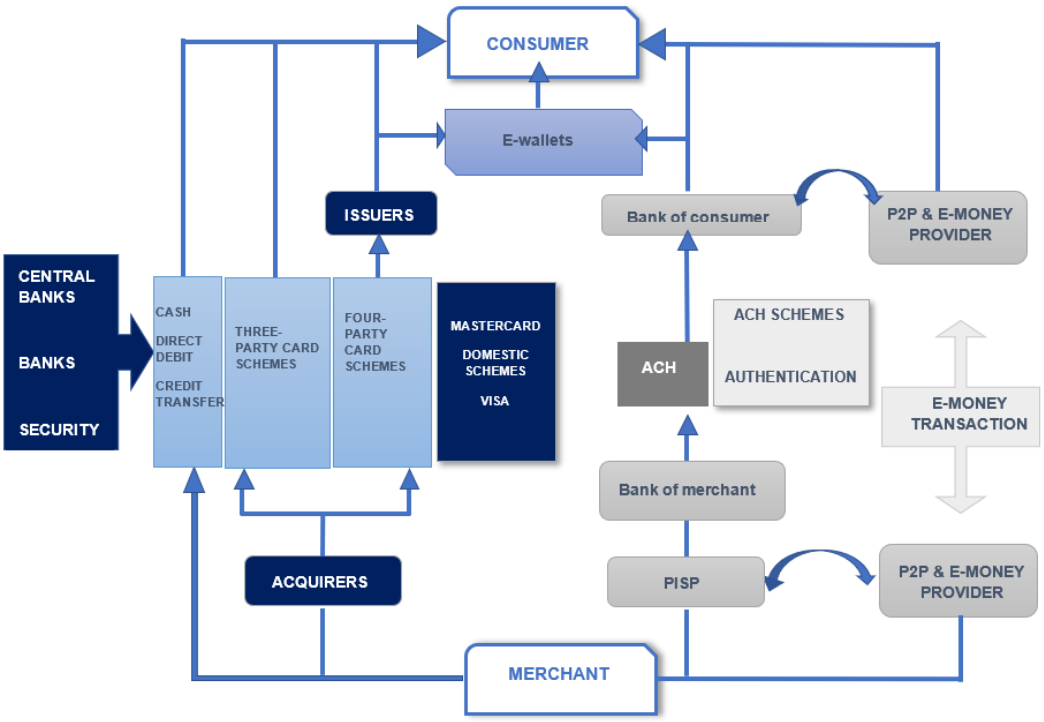
Source: Inspired by the diagram created by Oxera (2020)

Digital banking services, entry of non-banking players and the rising cost of bank operations have created the potential to affect "end-to-end manufacture and distribution" of payment products and services provided traditionally by banks. In fact, newly enabled interactions between supervised entities (credit institutions, electronic money institutions[40], payment institutions[41] and AISPs) and non-supervised entities (exempted companies, payment service providers' agents and electronic money distributors) have led to a growth in the number of market participants and a revamped value chain.

The growing presence and transaction value (see Section 3.1) of e-wallets and e-money represent one of the key changes in the value chain of payments, together with increased competition as a result of 'ACH' schemes (Automated Clearing Houses) which enable customers to pay via a PISP (as described above).[42] More specifically, technological developments (such as NFC and QR codes, see Section 3.4) and the penetration of smartphones and mobile payments (see section 3.1) have allowed non-supervised entities, such as telecoms operators, technology companies and smartphone manufacturers, to make new payment methods available via online payment methods and e-wallets and to put competitive pressure on the traditional payment value chain.[43] The figure below shows how technological advancement has created a new value chain.

[40] Introduced by Directive 2009/110/EC on electronic money ("EMD2")
[41] I.e. legal persons that have been granted authorisation in accordance with Article 11 PSD2 to provide and execute payment services throughout the Union. 'Payment institutions' included PISPs.
[42] Oxera (2020), The competitive landscape for payments: a European perspective
[43] Oxera (2020), The competitive landscape for payments: a European perspective

Figure 7: New payment value chain[44]



Source: Inspired by the diagram created by Oxera (2020)

Finally, it is worth noting that some merchants have included the delivery of their service along with the payment method, which can make it hard to distinguish between remote and in-store payments. In the case of Starbucks, for instance, it is possible to order and pay for a coffee through the app. Despite the payment being considered as a remote transaction, it also competes with traditional payment methods (such as cards or cash) that are used for in-store payments.

3.4. How widespread are new technologies used in the field of payments? Are there any potential obstacles to their further development? Which technological developments could be implemented in the long term?

As previously mentioned, **new payment processes**, such as **contactless cards** and new means of payment such as **mobile wallets** and **instant payments**, **are accelerating the move from cash to cashless payments** (EY & Copenhagen Economics, 2020). While the key innovation in the field of payment with regards to mobile payments started in the late 1990s[45], the level of adoption by consumers and merchants has been still limited.

Mobile payments, NFC and QR code technology

Mobile payments refer to payments done through a portable electronic device, such as a phone or a tablet. This technology can be used to send money using mobile devices from the initiation stage to the realisation of the transaction, and it includes confirmation and authorisation as well[46].

There are two broad types of mobile payment technologies: proximity and remote payments. When both parties are physically in the same location, it is referred to as proximity payments. In this case, communication between parties is done directly using contactless radio

[44] Merchants could provide payment initiation services only if they are licensed as PISPs
[45] https://www.primeindexes.com/indexes/prime-mobile-payments-index/whitepaper.html
[46] Ibid.

technologies. Remote payments, on the other hand, can be done irrespective of the payer's location, and are performed using a communication link, SMS, or a mobile application[47].

Proximity mobile payments have been spurred by the development and the growth of market share of two technologies: Near Field Communication (NFC) and Quick Response (QR) codes. NFC – which is a subset of radio-frequency identification (RFID, i.e. a technology that allows identification using radio waves)[48] – is a form of contactless communication between devices like smartphones or tablets. Contactless communication allows a user to wave the smartphone over an NFC compatible device to send information without needing to touch the devices together or go through multiple steps setting up a connection[49]. NFC technology in particular, tends to be considered as more secure and intuitive to consumers. In contrast to QR codes, it offers a secure element to prevent duplication and offer a product authentication. Unlike QR codes, NFC tags can be embedded into consumer goods. They are not discarded after a sale, they are a highly effective way to deploy engaging experiences throughout the entire customer journey. As a result, NFC in this way extends the value chain for a product.[50]

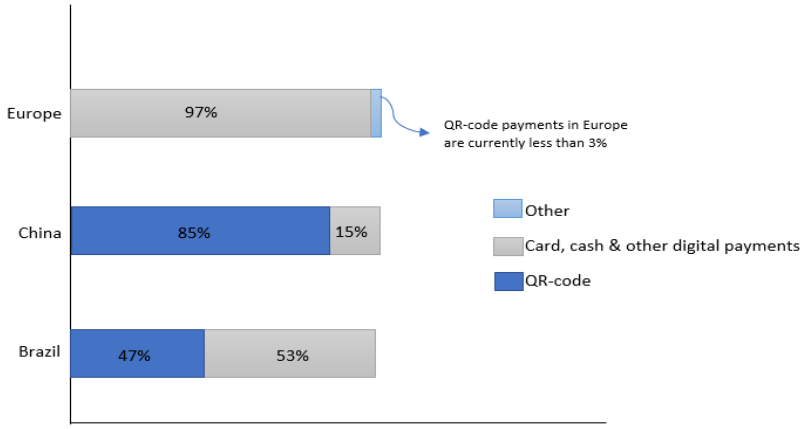
The most used cashless payment solutions in the EU are NFC-based, while other technologies, such as QR codes, are gaining traction more slowly. QR code technology works by scanning a barcode/QR code with a smartphone and the QR code prompts a specific action on the device, such as leading the user to an app or website for concluding the payment. The QR code can be generated by the merchant or by the customer's smartphone ('merchant-presented QR' or 'customer-presented QR'). For example, in the former case, for every transaction, a seller presents the QR code, which contains the relevant payment information, to enable its customer to make a payment. With a customer-presented QR code, instead of generating a unique QR code for every customer, the merchant is equipped with a QR scanner. Customers would then open their payment apps on their devices and display their personal QR codes. The merchant's scanner will read the code, then send a payment request for the purchase amount through the appropriate payment app. Non-bank PSPs are the main providers of QR code-based solutions; such as Swish in Sweden, Bizum in Spain, and iDeal in Netherlands (Hartmann et al., 2019; Kantar Public, 2022).

The adoption rate of QR codes in the EU is relatively low in comparison to Asian retail payment markets (3% of consumers in the EU, and 85% of consumers in China use QR-code based payment solutions) (Copenhagen Economics & Ant Group, 2022). In Europe, these are primarily based on domestic and international payment card schemes. QR code payments are seen as an efficient way to execute payments, through lower payment fees. This reduction arises from the underlying payment instrument: account-to-account payments, including instant payments, are a cheaper way of making payments than card or cash payments. With the Chinese economy growing rapidly, demand for efficient and convenient payment services grew at the same time.[51] Similarly, QR codes in India are becoming more popular, due to the low cost and low entry barriers it presents. An Indian merchant, for example, would only need a phone with internet connection and they're good to go running their business.[52]

According to Statista, **the market size of QR code transactions in Europe in 2020 was equal to USD 1.4 billion compared to more than 6 billion in North America and 2 trillion in the Far East and China.** This estimate is consistent with more recent research which observes that QR code payments are used by 85% of all consumers in China, whereas only 3% of consumers uses QR code payments in Europe[53].

47 Raina (2014), Overview of Mobile Payment: Technologies and Security
48 https://www.primeindexes.com/indexes/prime-mobile-payments-index/whitepaper.html
49 http://nearfieldcommunication.org/about-nfc.html
50 QR vs NFC (bluebite.com)
51 Copenhagen Economics (2022), Standardising QR code payments in Europe
52 NFC or QR payment? The endless debate | PaymentGenes
53 Copenhagen Economics (2022), Standardising QR code payments in Europe

Figure 8: Uptake of payment services in Europe, China and Brazil[54]



Source: Inspired by the work done by Copenhagen Economics (2022)

This low uptake of QR code payments can be explained by two main reasons. First, compared to the Chinese market, European consumers are well served by multiple payment solutions and services that are generally fast, cheap, secure and convenient to use: this implies that the possibility for new providers and new technologies to successfully scale is tough[55]. One additional factor also includes the fact that QR code payments are not as readily available as NFC at the POS, due to contactless card transactions.

Moreover, the European payments market is characterised by multiple and often purely domestic actors, leading to a fragmented market[56]. In fact, even where a mobile payment service operates in more than one country, they are typically limited to a small number of countries: no pan-European mobile payment solution or service currently exists outside the use of an international payment card in a mobile wallet. Indeed, under NFC in Europe, there tends to be a daily limit after which manually entering the pin-code is required. This defeats in some retrospect the purpose of a contactless payment. [57]

The use of QR code payments in Europe for closed-loop solutions, including loyalty programmes, such as scanning a membership card to access exclusive deals and perks, has gradually been increasing. An open European standard for QR code payments would provide the 'missing link' to address fragmentation and enable pan-European reach and interoperability of instant payments[58]. Factors that have been driving the current mobile-payment industry will continue to do so in the future, with some key observable trends: the demise of physical cards in favour of digital wallets, the growth of real-time/instant payments and the advent of digital currencies (these are further analysed below).

Introducing a European standard, by supporting the adoption of QR code technology, would also allow for the inclusion of European data protection, security, and cyber resilience standards in the QR code standard and interoperability design. [59] This is in line with the 2022 regulation on the "Digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014."[60]

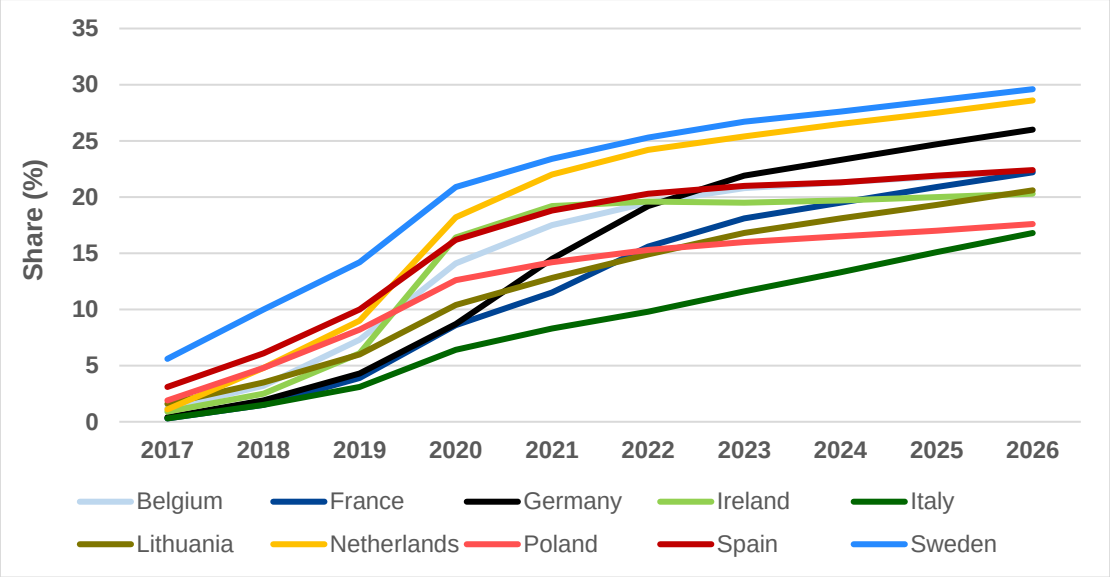
54 Proportion of adults using the service
55 Copenhagen Economics (2022), Standardising QR code payments in Europe
56 Ibid.
57 NFC or QR payment? The endless debate | PaymentGenes
58 Ibid.
59 Ibid.
60 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance)

As mobile wallet transactions are increasingly preferred by customers and merchants, QR codes adoption rates might increase in the near future (EY & Copenhagen Economics, 2020). In most Member States, customers who already adopted digital wallets would like to see the inclusion of QR codes not only for POS payments but also for scanning of bills and P2P payment such for splitting bills at social occasions (Kantar Public, 2022). What should be noted, however, is that in contrast to NFC, QR Codes may be easily duplicated and shared with others. Security risks may be high as they are not a good solution for sensitive applications and for anti-counterfeit.[61]

Digital wallets

Digital wallets (or e-wallets) are another disruptive innovation in the field of mobile payments. It all started roughly 10 years ago, when in 2011 Google launched Google Wallet, making it the first large company to provide a mobile wallet. With the wallet, consumers could make payments, earn loyalty points, and redeem coupons. In 2012, Apple introduced Passbook to be used for buying boarding passes and airline tickets. Apple Pay was launched in 2014, and Android Pay and Samsung Pay followed a year later[62].

Figure 9: Penetration rate of mobile POS payments in 10 Member States



Source: own elaboration based on Statista data, updated to March 2022

The figure above shows the penetration of mobile POS payments, i.e. transactions at point-of-sale (POS) that are processed via digital wallets[63]. In particular, the chart displays the penetration rate of mobile POS payments in 10 EU Member States.[64] With the exception of Spain and Sweden where the market share was sizable already in 2017, in the other countries, payments via digital wallets experienced a significant growth from close to 0% to an average of 14% of the market for digital payments[65]. Sweden and the Netherlands are the two countries with the highest penetration rate as of March 2022 (25.3% and 24.2% respectively). Overall, the data seem to suggest that the pandemic could have accelerated the use of this payment

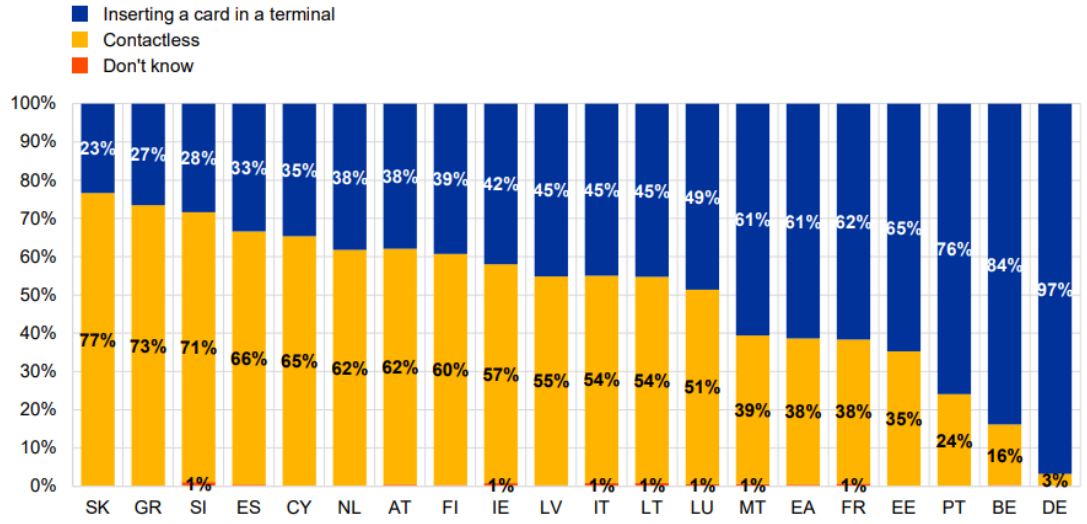
61 QR vs NFC (bluebite.com)
62 https://www.primeindexes.com/indexes/prime-mobile-payments-index/whitepaper.html
63 With payments processed via digital wallets we refer to a contactless interaction of a customer's smartphone app with a suitable payment terminal belonging to the merchant. The data transfer can be made, for example, via wireless standard NFC (Near Field Communication) or by scanning a QR code to initiate the payment.
64 Therefore, payment transactions with physical debit or credit cards at contactless terminals and mobile POS systems (e.g. Square, SumUp) as well as place-independent "Carrier Billing" are not included in this segment.
65 'Digital payments' do not include transactions between businesses (business to business payments) and payment transactions at the point of sale where mobile card readers (terminals) are used.

technology, as 2020 marked a sharp increase across the board. In terms of transaction value, mobile POS payments in the EU27 amounted to €4.2 billion in 2017, growing to €164.36 billion in 2021. Transaction value is expected to show an annual growth rate (CAGR 2022-2026) of 19.31% resulting in a projected total amount of €463.33 billion by 2026[66].

Contactless cards

The adoption of contactless cards varies across Member States. According to 2019 data from the ECB, 38% of the transactions finalised via card in the Euro Area (EA) were contactless (Figure 10):

Figure 10: Physical card payments (number of transactions)



Source: ECB (2019)

Contactless payments via physical card amount to the majority of card transactions in 13 out of 19 countries, and the euro area average is kept lower by strikingly low shares of contactless transactions in Germany (only 3%) and Belgium (16%). Contactless card payments, which are under €50 per transaction or the cumulative amount of the five previous consecutive transactions under €150, are exempt from the strong customer authentication (SCA) mandate of PSD2. However, the EBA (2021a) notes that low-value contactless payments may lead to an increased risk of fraud and liability issues as became evident in the DenizBank AG v *Verein für Konsumenteninformation* Case (Case C 287/19).

Instant payments

Instant payments are electronic payments that are processed instantly and allow the immediate transfer of funds from payers to payees. The European Payments Council (EPC) developed a pan-European instant payment scheme in 2016. The scheme is called SEPA Instant Credit Transfer (SCT Inst.) and based on the EPC's existing SEPA credit transfer (SCT) scheme (ECB, 2021c). **Instant payments are becoming increasingly available in the EU.** Over half of European PSPs offer services based on SCT Inst and the share of SCT Inst transactions in the total volume of SCT grew to 4.4% by the third quarter of 2019 (Baba et al., 2020). However, overall progress of SCT Inst has been below expectations. In December 2020, SCT Inst was used for just 8% of all SEPA credit transfer transactions, and its uptake varies across Member States (ECB, 2021c). According to Bundesbank, consumers do not see instant payment settlement as a necessity, although they would prefer to pay instantly when immediate credit transfer is required, such as in emergencies (Bundesbank, 2019).

[66] https://www.statista.com/outlook/dmo/FinTech/digital-payments/mobile-pos-payments/eu-27?currency=EUR

Instant payments in the EU were enabled in 2018 thanks to the launch by the Eurosystem of TARGET Instant Payment Settlement (TIPS), a market infrastructure service allowing payment service providers to offer fund transfers to their customers in real time and around the clock, every day of the year. This means that thanks to TIPS, individuals and firms can transfer money between each other within seconds, irrespective of the opening hours of their local bank[67]. Moreover, the EU Commission published a legislative proposal during the second half of 2022, which intends to address the currently fragmented market for cross-border real-time payments and provide a spur to Open Banking initiatives across the EU[68].

Digital and crypto-currencies

Finally, central banks' digital currencies – i.e. digital tokens or electronic records that represent the virtual form of a nation's currency – along with private sector cryptocurrencies are predicted to have the biggest disruptive impact over the next 20 years[69]. On one hand, scepticism within central banks about the potential of private sector cryptocurrencies to undermine the conduct of monetary policy is beginning to shift[70], and on the other hand 60% of central banks across the world are considering digital currencies, with 14% actively conducting pilot tests[71].

[67] https://www.ecb.europa.eu/paym/target/tips/html/index.en.html
[68] https://www.finextra.com/newsarticle/39668/eu-commission-to-legislate-for-full-eu-wide-coverage-of-instant-payments
[69] https://www.pwc.com/gx/en/industries/financial-services/publications/financial-services-in-2025/payments-in-2025.html
[70] Ibid.
[71] Bank for International Settlements (2021), Ready, steady, go? – Results of the third BIS survey on central bank digital currency

4. The review clause, Article 108

Under Article 108 of the PSD2, the Commission was required, by 13 January 2021, to submit to the European Parliament, the Council of the EU, the ECB and the European Economic and Social Committee, a report on the application and impact of the PSD2. However, the Commission had to postpone the review of the Directive due to its late transposition by some Member States[72] and the delay in the complete application of some of its provisions, in particular those contained in the Commission´s Delegated Regulation (EU) 2018/389[73] on strong customer authentication (SCA) and common and secure open standards of communication (access to accounts).

In addition to the general review (see Chapter 5), Article 108 of the PSD2 provides an explicit list of areas to be assessed. The aim of this specific list is to provide information on the implementation and application of the relevant provisions across the EU.

Each subsection in this chapter first provides a succinct introduction on the topic and a brief note on the transposition of the respective provisions. This is followed by key information on the implementation and application at national level and a conclusion. Information was gathered through desk research and a survey conducted with national representatives.[74] The analysis is limited by the fact that data on the practical application and impact of the provisions were not always available, partly as a result of late implementation, and stakeholders did not have strong views or knowledge of the provisions.

4.1. Appropriateness and impact of the rules on charges

Under Article 62(3) second setence of PSD2, “any charges applied shall by the payee to the payer must not exceed the direct costs borne by the payee for the use of the specific payment instrument”. According to Article 62(3) first sentence, “payment service providers shall not prevent the payee (e.g., the merchant) from (…) steering (the payer) towards the use of a given specific payment instrument”, by e.g., imposing charges or/and offering discounts.

Payees are thus allowed to apply surcharges, except for those payment instruments capped under the Interchange Fee Regulation[75] (as per Article 62(4)) in the case of two leg-transactions regardless[76] of the currency[77]. Surcharging is also forbidden for the payee in case of payment services to which the SEPA Regulation[78] applies, i.e., SEPA Direct Debit and SEPA Credit Transfers.

Article 62(5) further stipulates that Member States may prohibit or limit the right of the payee to request charges considering the need to encourage competition and promote the use of efficient payment instruments.

The surcharging ban applies:

[72] The European Commission opened infringement cases against, Latvia, the Netherlands and Sweden. See: Infringement decisions.

[73] 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, OJ L 69, 13.3.2018, p. 23–43.

[74] Member States taking part in the VVA survey on the PSD2 revision cover Belgium, France, Germany, Ireland, Italy, Lithuania, Netherlands, Poland, Spain, and Sweden.

[75] Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions, OJ L 123, 19.5.2015, p. 1–15.

[76] Payment transactions where both the payer’s payment service provider and the payee’s payment service provider are, or the sole payment service provider in the payment transaction is, located within the Union.

[77] See Article 2(4) of Directive (EU) 2015/2366.

[78] Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro and amending Regulation (EC) No 924/2009, OJ L 94, 30.3.2012, p. 22–37.

- to payment transactions where both the payer's payment service provider and the payee's payment service provider are, or the sole payment service provider in the payment transaction is, located within the Union; and
- when the consumer makes a payment using a consumer debit or credit card, or payment in euros using direct debit or credit transfer (known as SEPA payments)[79].

The surcharge ban also applies to B2B payments in euros made by business entities using direct debit or credit transfer, where the bank or card issuer of the business customer and PSP of the merchant are both located in the EEA. However, B2B payments made using a corporate credit or debit card can still be surcharged by law.[80]

Articles 62(3) to (5) of PSD2 have been transposed across the Member States. In this context, 15 Member States[81] made use of the option to further prohibit or limit the right of the payee to request charges within the transposition of Article 62(5) into national law.[82] Basically, charges for payment services are divided between the payer and payee with each responsible for the charges imposed by their payment service provider.

As far as the charges in Article 62(3) to (5) of PSD2 are concerned, where transposed, the subject matter of the provision is retaken into national law almost literally. Accompanying requirements have been introduced in some jurisdictions. For instance, an information obligation consisting of informing the payer before the initiation of the payment has been introduced in France[83] and in Belgium. As to the latter, the payer is to be liable for the charges only if it is aware of the full amount of the charge before the initiation of the payment transaction.[84] Specifically in relation to Article 62(4) of PSD2 (and its national transposition), the German Federal Supreme Court ruled that it is not a violation of the prohibition of surcharges for SEPA payment transactions if a merchant charges a fee for choosing the payment method 'PayPal' or 'Sofortüberweisung'.[85] In its ruling, the court held that the additional fees do not violate Section 270a BGB (local transposition of Aricle 62(4) of PSD2), since the additional fees were not charged for the credit transfer but rather for the involvement of a PSP that provides additional payment services and credit checks.[86]

There is no evidence of any official assessment on the appropriateness and the impact of the rules on charges conducted by a national authority. Similarly, no negative effects or impacts have been evidenced[87]. The sections on relevance, effectiveness and efficiency in chapter 5 provide further discussion of charging rules and the main conclusion from the evidence collected is that these rules are appropriate.

4.2. Limitations to 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

In accordance with Article 2(3), the PSD2 applies to intra-EEA payments, i.e., two-leg transactions where both the payer's PSP and the payee's PSP or the sole payment service provider in the payment transaction are located within the Union, in non-EEA currencies.

79 Emerchantpay, "Payment Services Directive 2 (PSD2) and SCA explained [2021 Update]"
80 Ibid.
81 For instance, Germany and the Netherlands. Concerning the latter, the rationale for non-transposition of Article 62(5) of PSD2 leans upon a conclusion that a complete ban on passing on costs does not promote the efficiency of payment transactions (VVA, 'National country report – Netherlands', 2022).
82 VVA, 'National country report – Germany', 2022, VVA, 'National country report – Netherlands', 2022.
83 VVA, 'National country report – France', 2022.
84 VVA, 'National country report – Belgium', 2022.
85 VVA, 'National country report – Germany', 2022.
86 The German Federal Supreme Court allows surcharges for certain payment transactions involving "Sofortüberweisung" and PayPal. Available at: https://www.jdsupra.com/legalnews/the-german-federal-supreme-court-allows-7990646/
87 In the 10 Member States covered in the in-depth analysis, namely Belgium, France, Germany, Ireland, Italy, Lithuania, Netherlands, Poland, Spain, and Sweden.

Moreover, Article 2(4) refers to payments where only one of the payment service providers is located within the Union to and from non-EEA countries (one-leg in or out) in any currency.

The jurisdictional scope of the SEPA Regulation extends beyond the EEA countries. Payments made in accordance with the SEPA Regulation and the SEPA Schemes, to or from countries and territories outside the EEA (e.g., Switzerland, Monaco, San Marino and the British Crown Dependencies) are one-leg transactions under PSD2.

It should be noted that the extension of the scope of PSD2 only applies to those parts of the transaction that are carried out within the EEA. By definition, PSPs cannot be in a position to fulfil their obligations in respect of transactions taking place outside of the EEA over which they do not have any control. Nevertheless, the PSD2 still applies to PSPs from outside the EU that transfer money into the EU.

Parts of Title III and IV are extended to non-EEA currencies and one-leg transactions as long as it is feasible for PSPs to comply with them. In particular, where a conversion between a currency different from the one of the payee's/payer's accounts is needed, conversions between an EEA currency and a non-EEA currency or two non-EEA currencies fall outside the scope of PSD2. Additionally, since PSD2 does not apply to the inter-PSP space, but to the PSU-to-PSP relationship, it is applicable only to the part of the transaction that is taking place within the EU[88].

In terms of the assessment of whether Titles III and IV could be applied in full to one-leg transactions (where technical feasible), the consulted stakeholders made only very limited contributions in the targeted consultation on the review of the revised PSD2[89]. **Overall, it is concluded that applying the PSD2 in this extra-territorial manner could create unintended consequences from a commercial and compliance perspective for PSPs and PSUs alike.**

Regarding the disclosure of currency conversion costs and any other information (such as the execution time) before and after a one-leg payment transaction, most of the participants in the targeted consultation expressed a negative position and suggested that technical and operational obstacles would make this approach unfeasible.

One of the technical issues in relation to ex-ante information concerns the case of "exotic" currencies, where such information is not accessible before the transaction is carried out. The reason for this, is that for some currencies, PSPs do not have a direct link with the service providers in charge of the foreign exchange transaction. It is therefore not possible to predict the turnaround times in such cases. Also, from an operational perspective, an EU PSP may not be able to specifically guarantee conversion rates for certain currencies (such as non-fiat currencies). Hence, it would not be possible to provide the estimated value of the transaction in the target currency for one-leg transactions as such an estimated value may not be accurate. If the estimate provided is not sufficiently precise, it is of little value to the consumer.

Specifically for the disclosure of execution time, the PSU is interested in the total execution time when the beneficiary will have the funds at their disposal. As there are no global agreements for execution times of incoming payments from other jurisdictions, this information is impossible to give. To base execution times on individual agreements between PSPs (mostly banks) would be very difficult and could lead to diminishing reachability of payments, since it is not feasible for a bank to have such agreements in place with hundreds of other banks. Without binding global agreements, information could be given for only a part of the execution time, and that could easily be misinterpreted by the customer and be considered misleading. In conclusion, without international payment systems being subject to the same regulatory

88 Ibid.
89 Targeted consultation on the review of the revised payment services Directive (PSD2)

standards as payment systems within EEA/SEPA, it is not operationally feasible for an EU PSP to guarantee a maximum execution time for one-leg transactions.

Also, from the legal and enforcement perspective, extension of Title III and IV obligations outside the perimeter of EEA/SEPA area could generate regulatory and integration problems with respect to countries that are currently outside this area, mostly due to global regulatory heterogeneity. A regulatory proposal to apply Titles III and IV to one-leg transaction could be appropriate only if done at an international level and with full reciprocity. If not, it could generate distortionary effects similar to the current disparity of obligations for intermediaries based in the EEA and those outside the EEA. However, setting the operational details of complex one-leg transactions which fall under different payments schemes and laws, might endanger the market-based approach (there could be disproportionate costs to banks and little benefits for PSUs if one-leg transactions are treated within the full scope of Title III and IV obligations).

Regarding the status quo of transposition, the limitations to the scope of application set down in Article 2(3) and (4) of PSD2 have been transposed into national law in full (retaking the literal wording, including the exceptions).[90] Hence, the scope of application per Article 2(3) and (4) is applied in compliance with the provisions of the PSD2 across all Member States. For issues other than the scope of transactions per se under the review clause, e.g., the scope of PSD2 in terms of impacted parties in payment services and other issues, see section 5.2 on effectiveness.

4.3. Access to payment systems and level of competition

Article 35(1) and (2) refer to access to payment systems, having regard in particular to the level of competition within the internal market. In principle, any PSP should be able to access the services of technical infrastructures of payment systems. The access is subject to appropriate requirements to ensure their integrity and stability.

For this purpose, the PSD2 set out dedicated provisions for the non-discriminatory treatment of payment institutions and credit institutions so that any PSP competing in the EU market is able to use the services of the technical infrastructures of those payment systems under the same rules and conditions. To ensure fair competition between PSPs, any participant in a payment system subject to the conditions of SFD (i.e., providing services in relation to such a system to an authorised or registered PSP) should grant access to such services in an objective, proportionate and non-discriminatory manner to any other PSP, if requested to do so.

In this context, it is also worth mentioning, that provisions relating to access to payment systems should not apply to systems set up and operated by a single PSP. These payment systems can operate in direct competition to other payment systems, or in a market not adequately covered by payment systems. They frequently include telecommunication providers providing payment services or internal systems of global banks where it would not appropriate to grant third parties access because it could hamper competition. Nevertheless, such closed systems are still subject to EU and national level competition laws which allows for granting access to these schemes to maintain effective competition in payments markets.

The criteria of non-discrimination and proportionality applicable to direct or indirect access to payment systems allow operators of payment systems to make informed decisions about access of direct and indirect participants, provided that access criteria are compliant with

[90] Member States taking part in a survey on the PSD2 revision, namely Belgium, France, Germany, Ireland, Italy, Lithuania, Netherlands, Poland, Spain, Sweden, confirmed that the scope limitation under Article 2(3) and (4) of PSD2 has been transposed into national law.

Article 35 of PSD2. Payment systems designated under the Settlement Finality Directive[91] continue to be exempted from the requirements of Article 35 (1).[92]

The exemption for three-party card schemes (3PS) from the access requirements does not apply to three-party card schemes that operate as *de facto* four-party card scheme (4PS), for example by relying upon licencees, agents or co-branding partners[93]. This was clarified by the CJEU in *Case C-643/16*[94], where the Court concluded that "a three party payment card scheme that has entered into a co-branding agreement with a co-branding partner does not lose the benefit of the exemption provided for by that provision and, therefore, is not subject to the obligation laid down in Article 35(1) of that Directive" in a situation where that co-branding partner is not a payment service provider and does not provide payment services within that scheme with respect to the co-branded products. However, a three-party payment card scheme that makes use of an agent for the purposes of supplying payment services loses the benefit of that exception and, therefore, is subject to the obligation laid down in Article 35(1)."

The PSD2 access requirement should be read in conjunction with Article 6 of the Interchange Fee Regulation (IFR) which provides that "any territorial restrictions within the Union or rules with an equivalent effect in licensing agreements or in payment card scheme rules for issuing payment cards or acquiring card-based payment transactions shall be prohibited". Therefore, a PSP permitted to acquire 3PS transactions in one EU Member State should also be allowed to acquire those transactions in other EU Member States[95].

Article 35 of PSD2 has been transposed into national law, including the conditions and exemptions.[96] In this regard, the transposed rules secure objective and non-discriminatory access while not inhibiting access more than is necessary to safeguard against specific risks, such as settlement risk, operational risk, business risk, and protecting the financial and operational stability of the payment system. In line with the PSD2, the limitations on access to the payment system cover, for instance in Germany, conditions concerning the functioning of the respective payment system (interoperability) and the payment system security.[97] Further, in Poland, the national provisions foresee that the payment system may not introduce restrictions on effective participation in other payment systems, rules that would introduce a difference in treatment between providers participating in different systems, based on the authorisation or lack thereof or on the basis of legal entity status.[98]

In general, **the provisions on access to payment systems (Article 35 of PSD2 as transposed into national law) are deemed to be essential for the market entry of payment service providers, they have fostered market entry and facilitated the creation of a level playing field**.[99] Chapter 5 provides additional detail with regards to the impact of PSD2 on PSP market entry.

4.4. Appropriateness and impact of the thresholds for payment transactions

Article 3(l) of PSD2 excludes payment transactions by providers of electronic communication networks or services provided in addition to electronic communications services for a subscriber, up to given limits, without the need to be authorised or registered. The goods and services that fall under the exclusion are digital content (e.g., music and digital newspapers),

91 Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems, OJ L 166, 11.6.1998, p. 45–50.
92 EBF Guidance.
93 Ibid.
94 Judgment of 7 February 2018, *American Express Co. v The Lords Commissioners of Her Majesty's Treasury*, C-643/16, ECLI:EU:C:2018:67, paragraph 69.
95 EBF Guidance. More precise source?
96 Member States taking part in a survey on the PSD2 revision, namely Belgium, France, Germany, Ireland, Italy, Lithuania, Netherlands, Poland, Spain, Sweden.
97 VVA, 'National country report – Germany', 2022.
98 VVA, 'National country report – Poland', 2022.
99 Based on information gathered from the Member States taking part in a survey on the PSD2 revision, namely Belgium, France, Germany, Ireland, Italy, Lithuania, Netherlands, Poland, Spain, and Sweden.

voice-based services (e.g., premium rate phone numbers), electronic tickets and charitable activity such as donations.

Physical goods do not fall within the exclusion. As the intention is for the exclusion to be used for lower-value and micro-payments, individual transactions are excluded only if they do not exceed EUR 50 and the cumulative value of payment transactions for an individual subscriber does not exceed EUR 300 per month.

The objective of this exemption is to ease the purchasing of tickets for an event or for transport through an electronic device as part of the provision of electronic communication services.[100] Recital 15 of PSD2 refers to services such as entertainment (chat, downloads, news and sport updates, directory enquiries, radio and TV participation such as voting) and Recital 16 provides examples of electronic tickets such as transport, entertainment, car parking and entry to venues.

Concerning the reference to charitable activity, Recital 16 states that "Member States should, in accordance with national law, be free to limit the exclusions to donations collected in favour of registered charitable organisations".

The specified threshold aims to limit the exclusion to payments with a low risk profile. Providers that leverage on the exclusion shall annually inform the competent authority of the results of a specific audit, testifying that the activity complies with the transactions amount limit set out in this provision[101].

Concerning the Member States, the exemption under Article 3(l) of PSD2 has been transposed into national law in full.[102] The wording was taken over literally or rephrased, but keeping the gist and scope of the exemptions, and where applicable, linked to related legal institutes under national law (for instance, on donations[103]); thus, no gold-plating is evidenced in respect of the exemption.

Similarly, the threshold applicable under Article 3(l) of PSD2 has been transposed into national law.[104] Possible inconsistency may stem from national adjustments, like for instance, in France, where, in the case of a subscription taken out for professional purposes, that amount is assessed at the level of an end user,[105] and in Germany, the threshold includes all taxes and, if applicable, shipping and other ancillary costs.[106] In this context, in Germany, the Federal Financial Supervisory Authority (BaFin) checks compliance with the cumulative threshold using a so-called 'statistical procedure' based on an average consideration of 'validly determined historical billing data'. The BaFin bases the statistical procedure not on subscribers, but on subscriber telephone numbers and differentiates between payment transactions with respect to the fixed telephone network and with respect to the mobile telephone network.[107]

There is no evidence to suggest that the threshold under Article 3(l) of PSD2 (and the same threshold under national law) is unreasonable. On the contrary, the threshold is seen as creating a reasonable balance between the interests of telecommunication service providers and customers in a practicable billing of value-added services on the one hand, and the interest in preventing the emergence of large-volume payment flows outside the regulated area on the other hand.[108] Further, there is no evidence that the threshold has any negative

[100] Ibid.
[101] Ibid.
[102] Member States taking part in a survey on the PSD2 revision, namely Belgium, France, Germany, Ireland, Italy, Lithuania, Netherlands, Poland, Spain, Sweden, confirmed that the exemption under Article 3(l) of PSD2 has been transposed into national law.
[103] VVA, 'National country report – France', 2022.
[104] Member States taking part in a survey on the PSD2 revision, namely Belgium, France, Germany, Ireland, Italy, Lithuania, Netherlands, Poland, Spain, Sweden, stated that the thresholds under national law tantamount that of Article 3(l) of PSD2.
[105] VVA, 'National country report – France', 2022.
[106] VVA, 'National country report – Germany', 2022.
[107] Ibid.
[108] VVA, 'National country report – Germany', 2022.

effects or impacts; in this context, the threshold has also not been subject to any national court rulings.

4.5. Appropriateness and impact of the threshold for Article 32 exemption

The derogation under Article 32 of PSD2 provides Member States with the option of exempting the application of most of the Title II prudential requirements for PSP that do not provide AIS or PIS; execute less than EUR 3 million worth of payment transactions a month; do not wish to sell or passport their services in other Member States; and can prove that none of the persons responsible for managing the business have been convicted of offences relating to money laundering, terrorist financing or other financial crimes (also referred to as "small payment institutions").

In addition, Article 14 stipulates that Member States must establish a public register of payment institutions including small PIs that are waived from the full authorisation requirements under Article 32.

The majority of the Member States have transposed the exemption under Article 32 of PSD2 into national law;[109] this is not the case, for instance, for Germany that did not avail the special regime for small payment institutions governed by the exemption.[110] A specific situation refers to Ireland, where the exemption under Article 32 of PSD2 has been transposed into a national piece of legislation, allowing the Central Bank of Ireland, as the national competent authority, to exempt payment institutions providing payment services under the determined threshold (which copies the threshold under Article 32 of PSD2). But the Central Bank of Ireland did not make use of that discretion;[111] as a result, no small payment institution waiver is applicable in Ireland. All payment institutions seeking to provide payment services in Ireland are required to apply for authorisation as a payment institution regardless of size or turnover.[112]

As to the threshold of the exemption under Article 32 of PSD2, most Member States[113] adopted the threshold as specified in Article 32(1) of PSD2, i.e. the monthly average of the preceding 12 months' total value of payment transactions executed by the entity concerned, including any agent for which it assumes full responsibility, does not exceed EUR 3 million per month and the requirements applicable on the natural persons responsible for the management or operation of the business. A minority of Member States introduced adjusted thresholds, though, none of those exceed EUR 3 million per month over the preceding 12 months. More specifically, for instance, in Belgium the threshold amounts to EUR 1 million per month over the preceding 12 months.[114] In Poland the transposition of waiver for small payment institutions refers to a new type of entity that was introduced, namely a small payment institution ("SMI"), as well as to a money services bureau ("MSB"). As to the former, the threshold applicable to SMI is set at EUR 1.5 million per month over the preceding 12 months; in addition, SMI providing a service of accepting cash may store no more than the equivalent of EUR 2 000 at a specific time in relation to an individual client. As to the latter, the average of the total amount of the payment transactions, including the transactions executed by MSB's agents, may not exceed the amount of EUR 0.5 million per month over the preceding 12 months.[115]

In practice, the application of the exemption under Article 32 of PSD2 within Member States' law has led to the introduction of special licensing regimes for small payment institutions, including the establishment of dedicated entities. In this regard, for instance in Belgium a 'light' regime for limited payment institutions and limited electronic money institutions has been put

[109] Member States taking part in a survey on the PSD2 revision, namely Belgium, France, Ireland, Italy, Lithuania, Netherlands, Poland, Spain, Sweden, confirmed that the exemption under Article 32 of PSD2 has been transposed into national law.
[110] VVA, 'National country report – Germany', 2022.
[111] Compare with the wording of Article 32(1) of PSD2 "Member States may exempt or allow their competent authorities to exempt […]".
[112] VVA, 'National country report – Ireland', 2022.
[113] Inter alia, France, Ireland, Italy, Lithuania, Netherlands, Spain, Sweden.
[114] VVA, 'National country report – Belgium', 2022.
[115] VVA, 'National country report – Poland', 2022.

in place, whereby the respective entities benefit from less stringent requirements on minimal capital levels, reporting procedures and internal control mechanisms, but they may not passport their service to other Member States. Similarly, in Lithuania the payment institutions may obtain a licence for the provision of limited services (limited licence payment institutions), whereby the payment institutions may not provide their services in other Member States.[116] A simplified authorisation for a payment institution not exceeding the threshold has been introduced in France, too; the respective institutions are not subject to the provisions requiring compliance with prudential standards.[117] In order to be registered as a small payment institution, a notification process is to be followed with an assessment by the Dutch Central Bank (the national competent authority). The process is similar to the licence application process, but with significantly less documentation to be submitted and less intense assessment by the Dutch Central Bank; the said process is not perceived as a simple registration, but as an application for a 'light' regime licence.[118] In Spain, a special register has been established for institutions below the threshold registering with the Bank of Spain (the national competent authority).[119] As already mentioned above, in Poland a new type of small payment institution – SMI has been introduced. An SMI is regulated and requires obtaining appropriate approval from the Polish Financial Supervision Authority (KNF; the national competent authority). The limitations applicable to SMI relate to the scope of services, as SMI may not provide services within the scope of initiating a payment transaction, nor services related to access to the account.[120]

The introduction of special regimes has not affected the level playing field (same business – same regulation – same risk) nor is there evidence that the special regimes hinder access to the market.[121] Nevertheless, the market of small payment institutions remains marginal. There were no licences issued for limited payment institutions in Belgium from 2019 to 2021,[122] while in Italy, the number is relatively low[123] and in the Netherlands, there are currently only 54 registered small payment institutions.[124]

The current threshold of EUR 3 million could be raised due to ongoing inflation of prices as well as the higher volume of processed transactions by small-scale PIs. As part of the quantitative assessment to set a new threshold due attention should be paid to the types of transactions to be included in or excluded from the calculation. The calculation of the threshold should be clarified (ideally EBA GL) and accompanied with concrete examples of underlying values to be used for the calculation with regards to the particular payment services (provide a methodology or at least a guidance for calculation).

Should the threshold be raised (either due to inflation in prices or an increase in the volumes of processed online payments by the small PIs), this could have a positive impact on the small PIs, especially those, which are close to reaching the threshold and would need to request a full-scale licence as a result. This could save the costs and time of obligatory licensing proceedings for small PIs (upgrade to standard PIs) and make them more competitive against standard PIs.

Overall, **the analysis concludes that threshold is still appropriate under current market conditions, but a limited increase to reflect inflation and market conditions could have a positive impact on smaller payment institutions and foster competition.**

116 VVA, 'National country report – Lithuania', 2022.
117 VVA, 'National country report – France', 2022.
118 VVA, 'National country report – Netherlands', 2022.
119 VVA, 'National country report – Spain', 2022.
120 VVA, 'National country report – Poland', 2022.
121 VVA, 'National country report – Belgium', 2022, VVA, 'National country report – France', 2022.
122 VVA, 'National country report – Belgium', 2022.
123 VVA, 'National country report – Italy', 2022.
124 VVA, 'National country report – Netherlands', 2022.

4.6. Possible introduction of maximum limits of amounts blocked on payer's payment account where the amount is not known in advance and funds are blocked

Article 75 relates to blocking of funds on a card-based payment account when the transaction amount is not known in advance. Where such payment transactions are initiated by or through the payee and the exact amount is not known when consent to execute is given, the payer's PSP should be able to block funds on the payer's account if the payer has given consent to the exact fund amount.

This provision, along with Recital 75, has been introduced to address card issues with pre-authorisations in some Member States where it can take up to several weeks for pre-authorisations to be cancelled or balances to be released by card issuers. When a purchase is made, a customer's card details are checked and the purchase transaction is authorised as normal, but the transaction is set to a 'pre-authorised' status. Funds may be placed on hold, and the money may not be debited to the card holder's account at this point but held until final payment is processed. Whether the amount is blocked or not depends on the agreement between issuers and cardholders. This, for example, may be the case when filling up with petrol at an unmanned gas station, in car rental contracts or when checking into a hotel[125].

Article 75(1) states that the issuer can only block an amount on the card if the cardholder has given his/her consent to the exact amount that can be blocked. Since it is the payee that has to inform the payer of the amount that he wishes to block on the card, the payer's ASPSP can only rely on the consent given by the customer to execute the transaction and therefore better specify customer's rights within the contract. In particular, the following could be considered in line with Article 75(1):

- If the amount to be blocked is displayed on the terminal screen (it is up to the terminal provider to provide for this) and the consumer types his/her PIN to consent to the blocked amount; and
- If the amount to be blocked on the card is communicated by the merchant to the cardholder in the form of a POS receipt (both physical and virtual POS) and the customer signs it/enters PIN to give his/her consent to the amount to be blocked[126].

In practice, the issuer in most cases will not have complete certainty that the amount was communicated by the payee to the payer. The issuer is reliant on the merchant's communication[127].

Pursuant to Article 75(2), the card issuer must release the blocked amount without undue delay after receipt of the exact amount and immediately after receipt of the payment order. Although the issuer is dependent on the merchant to advise the exact amount and cannot act without merchant co-operation, the latest the block will be released is when the issuer receives the payment order[128].

Article 75 of PSD2 has been transposed into national law across all Member States.[129] In general[130], there has been no evidence in relation to the necessity to complement Article 75 of PSD2 (or a transposed national provision) with maximum limits for the amounts to be blocked on the payer's payment account [131]. In this context, **the current amount and scope of Article**

[125] EBF Guidance.
[126] Ibid.
[127] EBF Guidance.
[128] Ibid.
[129] Based on information gathered from the Member States taking part in a survey on the PSD2 revision, namely Belgium, France, Germany, Ireland, Italy, Lithuania, Netherlands, Poland, Spain, and Sweden.
[130] A single departure from that approach refers to the Netherlands, where the blocked amount for transactions at gas stations will be raised to EUR 200 per transaction (VVA, 'National country report – Netherlands', 2022).
[131] Member States taking part in a survey on the PSD2 revision, namely Belgium, France, Ireland, Italy, Lithuania, Netherlands, Poland, Spain and Sweden.

75 of PSD2 provides a sufficient balance of interests between the economic need for security of the account holding payment service provider to reserve a sum of money and the need for transparency for the payment service user and to avoid the blocking of a disproportionate amount for a disproportionate time.[132].

[132] VVA, 'National country report – Germany', 2022.

5. Evaluation results

This Chapter provides an overview of the findings of the research per evaluation question. As set out in Chapter 2, specific questions, judgment criteria and indicators were developed for each dimension of the evaluation and these are presented in the evaluation matrix in Annex 9 of this report.

5.1. Relevance

The relevance section discusses the relation between the needs present at PSD2's inception and the objectives that were created to address them. In addition, the section looks at whether and how the needs have changed and might change in the future, and how the objectives of PSD2 address those needs. It does so by addressing three questions, namely:

- How relevant is PSD2 in light of market developments and given political priorities?
- How are the needs expected to evolve in the future?
- To which extent does PSD2 address current developments in the field of payment services?

In order to answer these questions the section draws on input from stakeholder interviews, European Commission publications and desk research. During stakeholder interviews interviewees were asked their views on PSD2's relevance, also with an eye on future developments. In addition, interviewees were asked other questions touching upon PSD2's relevance, such as on the licensing regime, SCA and the functioning of PSD2 APIs.

European Commission publications were used to assess what the problems and needs were that justified the revision of PSD2 as a follow-up to PSD1. Also, these publications are used to understand how the objectives were shaped in response to the needs and problems that PSD2 aims to address. Lastly, European Commission policy documents such as the Retail Payments Strategy (2020) were used to inform the policy priorities relevant to PSD2, and how those have changed since the introduction of PSD2.

Desk research further substantiates the findings from the stakeholder interviews and European Commission publications. Among other things, the desk research drew upon publications by national authorities, industry reports and policymakers' speeches.

The findings in this section have several limitations. The input from stakeholders is sometimes in the form of anecdotal evidence and it is not always substantiated by data. Moreover, the development of future needs, and the extent to which objectives will address them, remains uncertain.

5.1.1. How relevant is PSD2 in light of market developments and given policy priorities?

To answer this question, the needs relevant at the time PSD2 was initiated are first discussed. This is followed by the identification of needs that have emerged since then as well as continued and new market developments. Similarly, the changes in needs based on policy priorities are assessed.

Initial needs underpinning PSD2

There are seven main needs linked to payment services, their providers, and users that the PSD2 framework aimed to address:

1) Regulating the status of all payments service providers
2) More effective competition in certain payment areas
3) Fragmented market for innovative payment solutions
4) Harmonisation of licensing and supervisory rules and practices

5) More consistency in the application of PSD
6) Harmonisation of charging practices between Member States
7) Increased consumer protection

These needs link back to the main problems identified by the PSD1 impact assessment carried out before the introduction of PSD2 (EC, 2013). They link back to market failures and regulatory and supervisory gaps as observed during PSD1. These needs make up part of the broader intervention logic as described previously (see Annex 12).

Need 1: Regulating the status of all payments service providers

Since the adoption of PSD1, and prior to the adoption of PSD2, many innovative payment services had emerged on the market that were previously unregulated[133] (EC, 2013). These unregulated providers primarily offered payment initiation services (PIS) and account information aggregation services (AIS). For their services, these now considered third-party providers (TPPs) predominantly relied on "screen scraping", a technique through which the TPPs access bank accounts on behalf of customers using their credentials, potentially raising security concerns when static credentials were in place, consumer protection and competition issues[134]. In addition, the banks reportedly had difficulties telling whether the consumer, a TPP or other party was accessing the bank account.

Neither these services nor most of the providers were regulated or supervised. Thus, there was the need to regulate the status of these payment services providers and bring them within the scope of PSD2.

Need 2: More effective competition in certain payment areas

Prior to the adoption of PSD2, competition in certain areas of card and online payments was not always effective. Notably, in its impact assessment the Commission identified several restrictive business rules and practices which resulted in relatively high prices for card payments that were ultimately passed on to the consumers (EC, 2013).

The interchange fees charged by the issuers to acquirers for payment cards – regulated under the Interchange Fee Regulation (IFR) – made up a large part of merchant service charges[135]. Nevertheless, given the widespread usage of the cards and overall reluctance of merchants to turn down costly-but-popular payment instruments, this cost was ultimately passed on to the consumers either as a separate surcharge or through higher prices. This resulted in a competition that benefitted only some of the market players (banks, card schemes, acquirers) but disadvantaged others (merchants, consumers).

This was the main reason to consider the need to enhance effective competition in certain payment areas by addressing restrictive business rules and practices. This need was addressed by the implementation of both PSD2 and IFR, as well as antitrust enforcement.

Need 3: Integrated market for innovative payment solutions

Fragmentation of the payment services market along national borders has been one of the main problems that motivated the implementation of PSD2. At the time of PSD1, interoperability between different schemes was limited across EU Member States for card, online and mobile payments.

For card payments, the interoperability between different domestic card schemes was a large challenge. Many EU Member States had domestic card schemes (e.g., Girocard in Germany, Bancontact in Belgium). The bank cards for these schemes were a cheaper alternative to the international card schemes (Visa, MasterCard). Nevertheless, due to differences in standards

[133] Rec 4, PSD2
[134] For example, the unregulated payment service providers did not have to meet the same capital and liquidity requirements as regulated providers as well as were not required to offer the same safeguarding of funds or liabilities to consumers (EC, 2013).
[135] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R0751&from=EN

in different EU Member States the national cards could not be used in other countries at neither physical nor virtual terminals.

A similar situation was observed for online banking-based payment solutions. Due to national differences (technical standards, language, etc.) online banking service providers mostly focused on national markets. This substantially lowered interoperability between online banking-based payment solutions resulting in individual solutions being limited to the national level and only covering small clusters of banks (EC, 2013).

Fragmented markets prevent payment service providers from scaling up innovative, safe and easy-to-use payment services. This prompted the need to reduce the market fragmentation and spur innovation in the EU market for payment services.

Need 4: Harmonisation of licensing and supervisory rules and practices

Overall, ambiguity in the institutions in scope of PSD1 and the wide margin of discretion in the interpretation of PSD1 contributed to diverging licensing and supervisory practices in EU member states.

Licensing practices diverged primarily in speed and ease of obtaining the licence and supervisory practices diverged primarily in the interpretation of the exemptions under PSD1. This created many possibilities of arbitrage for payment institutions (PIs), effectively making it beneficial to be licensed in some Member States rather than others. For example, a large share of authorised PIs and e-money institutions were located in a single Member State, while a "huge majority" of exempted, smaller PIs were located in just two Member States[136].

The so-called "jurisdiction shopping" is problematic as PSPs can passport their services across EU Member States when they are licensed in at least one Member State. This creates challenges for supervision when the host Member State might be more stringent than the home Member State. This gives more market power to companies located in some jurisdictions vis-à-vis companies in other jurisdictions, leading to a distorted playing field. Indeed, the European Commission has found that many PIs made extensive use of passporting while being licensed in two/three Member States (EC, 2013). There was thus a need to harmonise the licensing and supervisory rules and practices.

Need 5: More consistency in the application of PSD

Similar to divergence in licensing and supervisory practices that prompted Need 4, many exclusions and exemptions introduced under the PSD1 were applied differently across EU Member States. This was predominately due to the wide margin of discretion in the interpretation of the PSD1 as well as the fact that exemption criteria were generally outdated. The main problems in consistency of the application of PSD1 exemptions were regarding commercial agents, limited networks, payments initiated by telco operators and independent ATM providers. The application of exclusions and exemptions in some Member States went beyond the intended scope set out in PSD1 and had the potential to increase risks for consumers.

Moreover, diverging application of PSD1 exclusions and exemptions also distorted competition in the payment market. For instance, diverging applications of the small payment institution exemption allowed for regulatory arbitrage. Large PSPs would establish several small legal entities to remain under the PSD1 thresholds in one country that allowed exemptions and passport their services to other EU Member States.

There was thus a need to ensure more consistency in the application of PSD.

[136] 224 out of 568 PIs and 30 out of 70 e-money institutions were licensed in the UK and a "huge" majority of 2 094 small PIs were located in Poland and the UK (page 27).

Need 6: Harmonisation of charging practices between Member States

Prior to the implementation of the PSD2 many merchants used surcharging to steer consumers to 'cheaper' payment methods, as some payments methods are more costly for merchants than others. A surcharge is a separate fee per transaction added on top of the price of a product/service which reflects the cost of the payment method.

The PSD1 allowed Member States to ban surcharging. This had led to significant heterogeneity with some member states banning surcharging, and others not. Diverging surcharging practices became a source of confusion for consumers especially with cross-border payments in the e-commerce sector.

In countries where surcharging was allowed, it was often not applied consistently or exploited by merchants:

First, not all merchants chose to surcharge even when allowed. This was due to the fact that merchants are required to accept all cards under the "Honour All Cards Rule" and the actual cost of transaction per payment method was not at all clear to the merchants.

Second, some merchants exploited the surcharging provisions applying excessive surcharges to increase their revenues. The European Commission found many examples where surcharging was significantly larger than actual costs borne by the merchant (EC, 2015).

There was thus a need to harmonise charging practices between Member States to enhance transparency on the market.

Need 7: Increased consumer protection

Due to the emergence of new payment solutions, increased digitalisation and the growing popularity of e-commerce, the security risks relating to electronic payments increased. Stakeholders developed customer authentication solutions to prevent fraud, but not in a harmonised way.

Moreover, consumer protection was particularly relevant considering the legal vacuum for the TPPs. Due to 'screen scraping' (explained above), banks often could not tell who was accessing the account: consumer, TPP or other party. This complicated protection efforts from the banks, for while they might have been able to detect that an account was being accessed by a scraper, they could not tell whether it was a malicious or benign scraper. There was thus a need to increase consumer protection.

The needs that underpin PSD2 follow from market developments and policy priorities before its inception. Yet markets have continued their development and policy priorities have changed. As a result the relevance of particular needs has changed and new needs have emerged.

Market developments

The market developments are split between, on the one hand, those already present at the time PSD2 was adopted and thus at least partially reflected in the needs, and on the other hand, those that have emerged since that might require new needs.

The market developments are those identified in the market developments section (see chapter 3) based on a literature review and stakeholder consultation.

Continuing market developments

The main **market developments** that were relevant before the adoption of PSD2 and remain relevant today are:

1) Fragmentation of payment services market;
2) Market penetration by innovative payment solutions;
3) Ineffective competition in certain areas of internet payments;
4) Diverging licensing and supervisory practices;

5) Increasing use of cashless and contactless payments; and
6) Diverging fraud rates and emergence of new types of fraud.

Each market development from the list and their relation to the needs underpinning PSD2 is discussed below.

Continuing market development 1: Fragmentation of payment services market

Overall, the payment services market remains fragmented along national borders, which means that due to a lack of standardisation and interoperability between different solutions most domestic payment solutions do not work across borders (EC, 2020).

In the realm of card payments, the problem is largely linked to interoperability issues between cards issued by the domestic and international card schemes, in the Member States where they are in place. The vast majority of the personal payment accounts come with a card of the domestic scheme in the countries where they operate. In principle, these cards can be used at any terminal in the EU. However, some European card schemes reported interoperability issues when carrying out contactless cross-border payments. The contactless feature of the POS terminals for cross-border payments is usually deployed by international card schemes (EC, 2020). The European Card Payment Cooperation is currently working on deploying the same feature for European card schemes, although that might take several years (EC, 2020). The inability to perform contactless payments with cards of domestic card schemes reduces their ability to compete with international card schemes domestically.

In parallel, when it comes to traditional 'chip and pin' card payments, to guarantee the acceptance of their cards for cross-border transaction, domestic card schemes rely to a large extent on their co-badging with international card schemes. In fact, a large majority of cross-border card payments in the EU is now made through international card schemes (ECB, 2019). In its recent Payment Strategy the Commission has vowed to reduce this dependency on the international card schemes and support the emergence of pan-European solution (EC, 2020).

In the realm of internet payments, individual solutions cover clusters of banks but are not interoperable across borders. Interviewed PISPs and AISPs emphasise that lack of standardisation and interoperability between different technical standards of the bank APIs hamper their ability to cover a larger number of banks. Setting up a connection to every bank is resource-intensive and an important reason for PISPs and AISPs to focus on a small number of national banks or make use of so-called aggregators (further discussed in new market development 8).

The following needs are affected as a result of the persistent fragmentation of payment services market:

1. The **need for an integrated market for innovative payment solutions** remains highly relevant – for instance, when it concerns contactless and digital payments as the market is still fragmented which stifles innovation.
2. The **need for more effective competition in certain payment areas** remains relevant as barriers to entry (such as limited interoperability) prevail and a substantial part of the EU payments market remains dependent on small number of international card schemes.

Continuing market development 2: Market penetration by innovative payment solutions

Since the adoption of PSD2 the uptake of innovative payment solutions has been rather limited. While European consumers increasingly show a preference for cashless payments, traditional banking cards remain the most-used payment solution in lieu of innovative payment solutions readily available on the market. In fact, for remote purchases, card payments make up approximately half of all purchases in terms of both volume and value. Digital payment solutions make up only about one quarter of all remote purchases (ECB, 2021). In its Retail

Payment Strategy, the Commission has highlighted that even within digital payment solutions, most of these solutions are still largely based on traditional cards or bank transfers (EC, 2020).

This is confirmed by the findings from the stakeholder interviews. Notably, the interviewed stakeholders mention that while new innovative payment services emerged on the market, the demand for innovative payment solutions has been rather limited, especially when it comes to consumer-oriented propositions. For example, PISP innovations have found little traction as merchants are having limited possibilities to steer customers to a cheaper payment method they are not familiar with. Merchants are, for instance, not allowed to provide a financial incentive in the form of surcharges for other payment methods. As for account information services, interviewed stakeholders report that new propositions, such as budgeting applications, are met with limited demand. Interviewed stakeholders stated that most successful propositions solve a "problem" that consumers are facing, and that AIS-based propositions so far have not done so – hence, modest demand.

The following need of PSD2 is affected as a result of the limited market penetration by innovative payment solutions:

3. The **need for more effective competition in certain payment areas** remains highly relevant as the competition of PSD2-enabled payment-initiation methods against traditional payment methods (card, cash) remains lacking.

Continuing market development 3: Ineffective competition in certain areas of internet payments

Different payment methods have different prices. Account-to-account payments, in the form of PSD2-enabled payment initiation services (for example by scanning a QR code) or domestic bank schemes, such as GiroPay, iDeal and Swish, are generally cheaper for merchants than card-based payments, such as debit cards and digital wallets based on cards from International Card Schemes and especially credit cards.

Ultimately, these transaction fees are aggregated and passed on to all consumers, unless surcharging is allowed. However, the majority of consumers are unaware of the costs behind each payment method. This information asymmetry might lead some consumers to make a sub-optimal choice: picking a more expensive payment method (credit card vs account-to-account) without the intention of using its services (chargebacks, insurance). As merchants incur higher costs because of consumers' choice for more expensive payment methods, prices for all consumers, including the ones not making use of these more expensive payment methods, would rise.

The following need is affected as a result of the ineffective competition in certain areas of internet payments:

4. The **need for more effective competition in certain payment areas** remains relevant due to information asymmetry, which results in consumers not having sufficient information to choose an optimal payment method. This often leads to increased transaction costs for merchants that are being passed on to the consumers.

Continuing market development 4: Diverging licensing and supervisory practices

Licensing and supervisory rules and practices remain divergent across EU Member States since the implementation of the PSD2. Regarding the licensing, practices within the EU diverge predominantly regarding the availability and clarity of the perimeter guidance, speed of the licence processing and regulatory replies. Interviewed stakeholders in some countries have mentioned that their national supervisors do not publish perimeter guidance and overall clarity is lacking when it comes to the regulatory communication surrounding PSD2.

Regarding supervision, the main diverging practice is not giving TPPs a possibility to open settlement accounts with the central banks. The interviewed stakeholders have underlined that accessing the clearing system through credit institutions is costly and challenging. When

opening a settlement account with credit institutions TPPs must pay a cost margin to the credit institution which makes their transactions more costly. Moreover, interviewed TPPs report that in some countries fewer and fewer credit institutions provide this service. Also, some TPPs recounted instances where credit institutions made the process of opening a settlement account unnecessarily lengthy and cumbersome due to their reluctance to provide such services to direct competitors. The European Commission is said to be aware of this issue and to be considering expanding the scope of the Settlement Finality Directive to include payment institutions (and e-money institutions), which could potentially resolve this issue.

In one EU Member State, Lithuania, the central bank allows TPPs to open settlement accounts and access the clearing system, thus making it easier for TPPs to do clearing. Nevertheless, in most other countries central banks do not have means or a mandate to facilitate clearing for TPPs.

Apart from settlement, interviewed stakeholders also pointed out diverging supervisory practices regarding the interpretation of key PSD2 concepts, such as the exact scope of payment services, definition of payment accounts and definition of excluded activities. Additionally, interviewed stakeholders noted an overall lack of effective coordination and communication between the national supervisors and EBA regarding the interpretation of PSD2 level 1 and level 2 text.

Diverging licensing and supervisory rules and practices create arbitrage opportunities for TPPs and ultimately facilitate so-called jurisdiction shopping. This leads to concentration of TPPs in one country. For those that are not based in this country are disadvantaged by the distorted level playing field. Moreover, it also creates challenges for the supervisors, where supervisors are not aware of how exactly the entity that is active in their jurisdiction via passporting is supervised in their home country.

The following needs of PSD2 are affected as a result of diverging licensing rules and practices:

5. First, the **need for harmonisation of licensing and supervisory rules and practices** remains highly relevant to ensure that market participants have the same level of supervision (ease of obtaining licence and intensity of supervision) regardless of where they are located.
6. Second, the **need for a more consistent application of PSD2** remains relevant to prevent jurisdictional shopping and provide a level playing field across the European Union.

Continuing market development 5: Increasing use of cashless and contactless payment methods

The Covid-19 pandemic triggered a substantial increase in cashless payments. Due to hygiene concerns, consumers increasingly used electronic payments rather than cash. The trend of switching cash payments for electronic payments was already visible before Covid-19 (ECB, 2021), but the pandemic has substantially accelerated it. Before the pandemic, the convenience, speed and security of electronic payments compared to cash payments drove the switch from the former to the latter. Both before and during the pandemic, electronic payments increasingly took the form of contactless payments.

The following needs of PSD2 are affected as a result of the growing preference of consumers for cashless and contactless methods:

7. First, the **need for increased consumer protection** remains relevant as security of payment remains one of the main priorities for consumers when choosing a payment method. As a switch to a new payment method (contactless) takes place, continued attention to consumer protection remains paramount.

8. Second, the **need for an integrated market for innovative payment solutions** remains relevant as the interoperability of payment solutions remains one of the main priorities for consumers when choosing a payment method.

Continuing market development 6: Diverging fraud rates and emergence of new types of fraud

Since the implementation of PSD2, the fraud rates have somewhat diverged. Overall, according to interviewed stakeholders, no substantial increase in fraud rates has been witnessed and fraud rates are generally low.

Some of the interviewed stakeholders, predominately large merchants, have said that they did not witness a significant reduction in online fraud rates since the implementation of PSD2 as it was already low before. Other interviewed stakeholders, notably TPPs, have also noted that the developments in fraudulent transactions diverge across countries – in western EU countries the fraud rate did not change as most stakeholders already had some sort of fraud prevention in place, while in other countries the fraud rates have gone down since the implementation of PSD2.

Nevertheless, new types of fraud have emerged on the market following the rise in online shopping and cashless payments due to the Covid-19 crisis. The main new payment threats and fraud enablers include social engineering, phishing, malware, advance persistent threats, denial of service, botnets and monetisation channels (European Payments Council, 2021), which is primarily relevant for the evolution of SCA.

The following need is affected as a result of the diverging fraud rate developments and the emergence of new types of fraud:

9. The **need for increased consumer protection** remains relevant insofar as it concerns the emergence of new types of fraud on the market. Concerning already existing types of fraud the need has now become less relevant as fraud rates either remained low or substantially decreased across EU Member States.

New market developments

In addition to the continuing market trends, the following new market trends have taken between the adoption of PSD2 and mid-2022:

1) Emergence of premium APIs;
2) Emergence of API aggregators;
3) Emergence of 'licence-as-a-service' providers;
4) Entry of BigTechs to the payments market;
5) Growth in account-to-account payment services;
6) Growth of digital wallet services; and
7) The rise of buy-now-pay-later services.

Each new market development from the list and their relation to the needs underpinning PSD2 is discussed below.

New market development 1: Emergence of premium APIs

PSD2 introduced the requirement for ASPSPs to either create APIs that allow licensed parties to access account information and initiate payments on behalf of their customers, or to allow the use of the interface for the identification and communication with the account servicing payment service providers' payment service users. In addition, some ASPSPs have ventured beyond the PSD2-mandated APIs and introduced a set of so-called premium APIs[137]. Through premium APIs, parties wanting to offer AIS and PIS services have access to functionalities

[137] https://www.yolt.com/open-banking/premium-api

beyond the ones mandated by PSD2. For example, premium APIs may provide transaction information from other additional type of accounts (e.g., savings accounts), allow the initiation of batch payments and access account information more than four times per day. In exchange for the access to the premium APIs, ASPSPs charge a fee.

Crucially, the access of PSD2-mandated APIs requires the party offering AIS or PIS services to possess a PSD2 license – i.e. to be a TPP – which is according to the interpretation of at least some market participants not required for the services not required under PSD2 and only accessible through premium APIs. Since premium APIs fall outside the scope of PSD2 for those services, the premium access provided by the ASPSP to the party wanting to offer AIS or PIS services is governed by a bilateral commercial agreement. While this agreement must respect GDPR rules and specific domestic legislation for the banking sector, PSD2 standards and licence requirements are not applied to these additional services.

Indeed, premium APIs offer an unlicensed party the option to access exactly what is contained in the PSD2-mandated API (plus some more). In practice, therefore, a party offering AIS or PIS services is confronted with the choice of (1) obtaining a PSD2 licence and facilitating AIS or PIS services as a TPP under PSD2 or (2) in addition concluding bilateral agreements with ASPSPs offering premium APIs and being able to offer the same or additional services without TPP licence (as discussed in new market development 3, a third option is to use the 'licence-as-a-service' model).

Obtaining a PSD2 licence is a resource-intensive process for prospective TPPs. Moreover, TPPs must comply with AML requirements. While accessing premium APIs comes with a cost, unlike accessing PSD2-mandated APIs, parties using premium APIs do in most instances not obtain a PSD2 licence or comply by its AML requirements. As a result, an uneven playing field is created: two parties offering the exact same service operate under different conditions. While at best the two parties incur similar costs yet allocate them differently, at worst this system gives unlicensed parties a competitive advantage. This might lead to potential lack of clarity for market players about the need to obtain a licence: an interviewee noted that competitors in its Member State had given up their PSD2 licence and continued to operate through premium APIs.

The following needs are affected as a result of the emergence of premium APIs.

- First, the **need to regulate the status of all and clarify the legal framework applying to payment service providers** remains highly relevant since the introduction of premium APIs has effectively created a class of unlicensed TPPs that might have led to a lack of clarity for market players about the need to obtain a licence.
- Second, the **need for more effective competition in certain payment areas** remains relevant as the emergence of premium APIs might results in licensed and unlicensed parties competing with one another show a need to go beyond the 'basic access' covered under PSD 2.
- Third, the **need for increased consumer protection** remains relevant as customers of unlicensed parties making use of premium APIs do not enjoy the protection that customers of a licensed TPP do. Consumers may be less protected in case of fraud or misappropriation of funds, lower technical security standards and less transparency on costs. Moreover, consumers may not be aware of these risks, as they may not be able to differentiate between licensed and unlicensed parties.

New market development 2: Emergence of API Aggregators

Since the introduction of PSD2 a new type of service has emerged called the (API) aggregator[138]. Aggregators are PSD2-licensed parties that build a single API on top of many

[138] Over 15 API aggregators are headquartered in the EU at the time of writing: https://www.openbankingtracker.com/api-aggregators

other APIs. Given the lack of a PSD2 API standard and the proliferation of ASPSP APIs that followed, aggregators provide a single access point to a large number of ASPSP APIs[139]. Aggregators can therefore be thought of as a market solution to the absence of a PSD2 API standard and the large number of APIs.

Aggregators operate in two modes, as a TSP and TPP.

As a TSP, aggregators provide the 'rails' which TPPs use to easily connect to a large amount of ASPSP APIs. Through their own API – a single access point – aggregators allow TPPs to easily access account information and initiate payments at a variety of ASPSPs. In exchange for a fee, the TPP saved the effort of implementing a proprietary solution for each individual ASPSP to which it wants to connect. Since the aggregator functions as a TSP and only provides the rails, the ASPSP will identify the TPP as making the API calls and AML compliance lie with the TPP.

As a TPP, aggregators can provide the AIS and PIS services to parties without a licence can connect to the aggregator and use its licence and rails to access account information and initiate payments. This service is known as licence-as-a-service (see new market development 3). When operating as a TPP, the ASPSP will identify the aggregator as making the API calls and is not aware which party it is requesting the data or initiating the payment on behalf of. As the licensed party, the aggregator is responsible for AML compliance and the consumer will give consent to the aggregator.

The following needs are affected as a result of the emergence of (API) aggregators (excluding the licence-as-a-service related aspects):

- First, the **need to clarify the legal framework regulate the status of all payment providers** remains highly relevant as aggregators operating under a PSD2 licence provide a technical service which was not envisioned as such under PSD2.
- Second, the **need for more effective competition in certain payment areas** remains highly relevant as aggregators have become, among other things, the paid-for alternative to a PSD2 API standard. Instead of connecting to several free ASPSP APIs, new entrants therefore must choose between costly implementation of proprietary connections or pay service costs to an aggregator. Either way, these costs increase the cost of market entry for new payment solutions and increase the costs of offering payment services, reaffirming the relevance of more effective competition in certain payment areas.
- Third, the **need for increased costumer protection** remains relevant as the pass through of customer data through an additional system has the potential to make it more difficult to ensure the safety of consumer's accounts as well as the data stored on it. Indeed, ASPSPs will not always have sight on which TPPs ultimately use the customer data or initiate a payment when it is transmitted through an aggregator, which interviewed ASPSPs note as a limitation to their ability to protect the consumer.

New market development 3: Emergence of 'licence-as-a-service' providers

Similar to the API aggregator proposition, the licence-as-a-service proposition is a new proposition that has emerged since the introduction of PSD2. In essence, a party without a licence that seeks to access account information or initiate a payment (as part of its service offering) asks its customer to give consent to the licensed TPP to access account information or initiate a payment on its behalf. The TPP whose licence is used is the party that is given consent to, complies with AML requirements, and identifies itself when making an API call at an ASPSP. The information is then passed on to the unlicensed party.

Two types of licence-as-a-service models can be distinguished.

[139] Bridge.io, a French aggregator, for example connects to over 200 banking institutions: https://bridgeapi.io/en/bridge-aggregation. Other examples include Ibanity, Salt Edge and Yolt.

The first type of licence-as-a-service model is one where TPPs provide unlicenced parties services in which the TPP accesses the consumers information and provides a service to the unlicensed party derived from the obtained information. For example, a TPP may provide a loan provider an assessment or advice regarding the loan suitability of a customer based on its transaction history. In this model, the TPP provides a service based on the data it can access, without transmitting the original information from the ASPSP.

The second type of licence-as-a-service model is one where the TPP simply hands over the data or initiates the payment that the unlicensed party would have done itself had it possessed a license. AIS services may use such a service to obtain the transaction history of its customer or PIS services may use it to allow customers to initiate payments from, for example, their app. API aggregators may offer this service to unlicensed parties as an alternative to the rails they provide to licensed parties (see new market development 2). Mixed models, which combine elements from both models, may also exist.

TPPs that provide licence-as-a-service models are in effect a middleman for the data or payment initiation that unlicensed parties want to provide. Certain risks may emerge from this construction. First, it is unclear if the customer is fully aware of which party it's giving consent to access its data. The party which the customer consents to is a different from the party offering the service to the consumer. Second, ASPSPs do not have sight on which unlicensed party is provided the account information or facilitating the initiation of a payment. Third, the unlicensed party that obtains the data or facilitates the initiation of a payment is not supervised as a TPP under PSD2.

The following needs are affected through the emergence of licence-as-a-service providers:

- First, the **need clarify the legal framework regulating the status of all payment service providers** remains highly relevant, as the licence-as-a-service model, like premium APIs, might have led to lack of clarity for market players about the need to obtain a licence has in effect created a class of unlicensed TPPs.
- Second, the **need for more effective competition in certain payment areas** remains highly relevant as the emergence of the licence-as-service model might show a need to go beyond the 'basic access' covered under PSD 2 that results in licensed and unlicensed parties competing with one another. Seeing that licensed parties (TPPs) must comply with PSD2 standards whereas unlicensed parties do not, TPPs compete on an uneven playing field.
- Third, the **need for increased consumer protection** remains relevant as consumers are not necessarily aware of the PSD2 licensed and supervised entity as well as enhanced risks with the involvement of non PSD2 licensed entities.

New market development 4: Entry of BigTechs to the payments market

Since the introduction of PSD2, BigTechs have become sizeable and visible players on the European payments market. AliBaba, Amazon, Apple (e.g., Apple Pay), Google (e.g., Google Pay for Android devices), Facebook and Tencent are developing and promoting their payment solutions on the EU market.

What unites BigTechs in their desire to enter the European payments market is that they operate platform-based digital ecosystems. Providing payment services within these ecosystems is lucrative and further allows them to leverage important network effects[140]. BigTechs are therefore in a strong position to challenge established players. Yet concerns about their market power exist. The European Commission has outlined such concerns in its Retail Payments Strategy, in which it stated the aim to maintain a level playing field for all players (i.e. BigTech, incumbents, or other new entrants[141]).

[140] https://www.suerf.org/suer-policy-brief/29669/digital-payments-and-european-sovereignty
[141] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0592&from=EN

The following needs are affected as a result of the entry of BigTech to the payments market:

- First, the **need to regulate the status of all payment service providers** remains relevant as large technology firms may operate outside, or within exemptions, of PSD2. For example, by offering their own stablecoin, or by operating as a TSP. Yet as their role in the payment market grows, and their services affect monetary sovereignty and financial stability, further regulation and supervision may be warranted.
- Second, the **need for more effective competition in certain payment areas** remains highly relevant. BigTechs benefit from network effects and wield market power. While this can instantly make them formidable competitors to established players, network effects and market power which may distort the level playing field, preventing effective competition.
- Third, the **need to strengthen the autonomy and resilience of the European payments market** becomes more relevant (See description of this new need below). BigTechs play an increasing role on the European payments market through their digital wallets and online ecosystems.

Need 8: Strengthening the resilience and autonomy of the European payments market

The need to strengthen the resilience and autonomy of the European payment market has emerged in recent years in the context of the broader policy debate about economic resilience and strategic autonomy (EC, 2020).

Already at the start of the current Commission's term the development of European financial market infrastructure and its resilience was identified as a priority[142]. US sanctions towards Iran and the Nord Stream 2 pipeline confronted European policymakers with the continent's reliance on foreign financial infrastructure, and the loss of financial sovereignty that it brought about.

More recently, the Council reaffirmed the strategic importance of an autonomous European financial sector. With regards to the European payments market, it singles out the importance of a homegrown, pan-European, market-based payments solution. In addition, the importance of open and autonomous European payments area is emphasised[143].

The potential impact on resilience and autonomy of the European payments market is thus a relevant need to consider for potential revisions of the retail payments legislation.

New market development 5: Growth in account-to-account payment services

Account-to-account payments, direct credit transfers from one bank account to another, are rising because of the PIS services PSD2 enabled and domestic account-to-account schemes.

PIS (see also Future development 3.) allow one party to initiate a payment at the bank of another party. For example, for a merchant to initiate a payment at the bank of a customer. Generally, this lowers the costs of the transaction and increases the speed, especially when compared to (credit) card schemes. While the merchant initiates the payment, the customer will have to confirm the transfer in its own banking environment – e.g., through an app on its phone.

Account-to-account payments are also driven by domestic efforts within Member States. Schemes, such as Giropay (Germany), iDeal (Netherlands), Swish (Sweden) and Bizum (Spain), facilitate account-to-account payments across the major banks in the respective countries. Concurrent with the rise in e-commerce and a shift away from cash, these services are seeing the number of payment transactions they process increasing.

The following needs are affected by the increase in account-to-account payment services:

142 https://www.europarl.europa.eu/legislative-train/theme-a-stronger-europe-in-the-world/file-eu-financial-sovereignty
143 Conclusion 34: https://data.consilium.europa.eu/doc/document/ST-6301-2022-INIT/en/pdf

- First, the **need to regulate the status of all payment service providers** remains relevant as domestic account-to-account schemes are generally operated by established ASPSPs. While other parties may be able to opt-in, the scheme is in essence a closed alternative to the PIS services PSD2 prescribes. As these schemes fall outside the scope of PSD2 but provide payment services similar to those that do, the need to regulate the status of all PSPs remains relevant.
- Second, the **need for more effective competition in certain payment areas** remains relevant as domestic account-to-account schemes owned by ASPSPs compete with PSD PISs on a somewhat uneven playing field. ASPSPs account-to-account payments may benefit from better integration and promotion within ASPSPs' banking environments. They are able to capitalise on a recognisable brand and gain trust from their affiliation with ASPSPs, with whom most users have a long-standing relation. In turn, PIS providers do not benefit from the network effects, recognisability and promotion that competing, ASPSP-owned, account-to-account schemes benefit.
- Third, the **need to resolve the fragmented market for innovative payment solutions** remains relevant as the domestic account-to-account payment schemes entrench payments within national borders and will do so further as they become the dominant mode to settle account-to-account payments within Member States.

New market development 6: Growth of digital wallet services

Digital wallets store virtual copies of existing debit or credit cards. Popular examples in Europe include Apple Pay and PayPal. With their digital wallet, consumers can pay with a virtual debit or credit card at a POS or online. Digital wallets work through QR codes, Magnetic Secure Transmission, Near Field Communication or an online login. The latter two options are most common when paying in store (NFC) or online (online login).

Digital wallets provide a convenient alternative to using physical debit or credit cards for customers when paying at a POS, or banking interfaces when paying online. Besides doing away with the need to carry a physical card, digital wallets let customers authorise payments just as they would unlock their phone, such as through a finger scan, face scan or entering a password.

As such, digital wallets are often considered a more convenient method of payment. Digital wallets, such as Apple Pay or PayPal, combine two elements of SCA, the having of something (a phone, a laptop) with the knowing of something (password, in the case of PayPal) or the being of something (biometrics, in the case of Apply Pay). In practice, this means that when completing a payment from a known device, the consumer only has to enter the password or verify the biometrics to complete the purchase. This is often a smoother process compared to an online card transaction. In general, an online card transaction must be confirmed in the app from the bank the consumer is using. This implies switching to a different app when on a mobile device or switching to a different device when completing an online purchase on a laptop or PC.

The ease of digital wallets therefore provides consumers with an incentive to use them. Yet while convenient in use, they can be more expensive, too[144]. As such the further uptake of these wallets can drive up costs for merchants and indirectly consumers.

Also, the operators of digital wallets are often considered TSPs and do not require a PSD2 licence for their operations[145]. As digital wallets compete for payments with parties that do need to possess a PSD2 licence, such as card providers or PIS providers, not having to possess a licence and being compliant with PSD2 can be a competitive advantage.

[144] A PayPal transaction, for example, is often more expensive than an account-to-account or card-based payment, as shown in Continuing market development 3.
[145] Apple, for example, is not required to hold a PSD2 licence in order to offer Apple Pay to customers.

The following needs are affected through the growth of payment wallet services:

- First, the **need to regulate the status of all payment service providers** remains highly relevant as providers of digital wallets may operate without a PSD2 licence or benefit from exemptions[146], providing important payment services without being under PSD2 supervision.
- Second, the **need for more effective competition in certain payment areas** remains relevant. Digital wallets may compete for payments with card schemes or PIS providers, without having to possess a PSD2 licence and fulfil its compliance requirements. As a result, they may have a competitive advantage when competing for payments.

New market development 7: The rise of buy-now-pay-later services

Buy-now-pay-later (BNPL) services allow a consumer to make a one-time payment in instalments, without borrowing costs. When completing a purchase, BNPL options are presented alongside regular payment methods such as cards and digital wallets. Merchants, who bear the cost for the consumers' borrowing in the form of higher fees, may offer BNPL options to increase conversion rates and provide for a payment service demanded by customers.

The number of payments concluded through BNPL services is growing fast[147], especially in sectors such as clothing and footwear[148].

The following need is affected through the rise of BNPL services:

- The **need consumer protection** remains relevant as buy-now-pay-later services provide consumers with an easy and speedy way to pay for goods (while getting into debt). The ability of a consumer to service debt is not considered when completing the purchase, and consumers might not be aware of the terms applied and costs invoked when an instalment is missed or paid late.

Policy developments

In addition to the market developments, the main developments related to the EU's policy priorities relevant to PSD2 relate to:

1) Opening restricted technical infrastructure;
2) The push for a pan-European payment solution; and
3) The push for implementation and adaptation of instant payments.

Each political development from the list and their relation to the needs underpinning PSD2 is discussed below.

Policy development 1: Opening restricted technical infrastructure

Mobile devices are crucial in facilitating electronic payments; digital wallets are often stored on them. When at a POS, a consumer can rely on its mobile device to exchange and verify payment information with the merchant in a fast and secure manner. This is done through the technical infrastructure present on the mobile device of the consumer, generally in the form of a Near Field Communication (NFC) chip. Access to this infrastructure is therefore of vital importance to PSPs, offering digital wallet services on mobile devices.

PSPs do not always have access to the technical infrastructure on mobile devices. For example, PSPs do not have access to the NFC chip on Apple devices. Consumers with an

[146] PayPal, for example, does not possess a PSD2 licence. Others, such as Apple, do, but are excluded from the scope.
[147] https://www.nets.eu/perspectives/Pages/How-European-banks-can-benefit-from-Buy-Now-Pay-Later.aspx
[148] https://www.mckinsey.com/industries/financial-services/our-insights/buy-now-pay-later-five-business-models-to-compete

Apple device are therefore left to choose from Apple's own digital wallet when wanting to use the conveniences of the NFC chip.

Recently, the European Commission has signalled a willingness to tackle this issue. In its Retail Payments Strategy (2020), the European Commission states that innovative payment solutions should be able to use all relevant technical infrastructure. More recently, in May 2022, the European Commission informed Apple of its preliminary view that it abused its dominant position in markets for mobile wallets on iOS devices by limiting access to standard technology (the NFC chip in iPhones) used for contactless payments in stores[149].

The following need is affected through the political prioritisation of opening restricted technical infrastructure:

- The **need for more effective competition in certain payment areas** may be impacted by the competition proceedings launched by the European Commission. These would be expected to improve competition in digital payment wallets. The need for additional measures that aim to ensure effective competition, or to facilitate it, would therefore become less relevant.

Policy development 2: The push for a pan-European payment solution

Since the introduction of PSD2 the need for a pan-European payment solution has taken on renewed urgency. An increasing reliance on non-European card schemes for cross-border transactions and the compliance of those card schemes with US sanctions has reminded policymakers of the threat they pose to European sovereignty. Moreover, fears exist that these schemes create what is in effect a duopoly, harming competition and consumer welfare.

Previously, domestic card schemes reigned supreme, providing Europeans with relatively cheap methods of payments albeit ones restricted to national borders. Over the last 20 years the number of domestic card schemes has decreased. Recently, the exit of domestic schemes from the market stopped, and these schemes have kept stable market shares since the years that followed the implementation of the Interchange Fee Regulation, as analysed in the European Commission's June 2020 report on the implementation of the IFR (European Commission, 2020). In spite of this, currently, over half of transactions are conducted through international card schemes. Most EU countries currently rely entirely on Visa and Mastercard for the processing of their domestic transactions.

Yet Mastercard and Visa are US-based companies and abide by restrictions put in place by the US government, even when those payments are initiated and completed abroad. For Europe, this carries a loss of (financial) sovereignty, as payments to and from certain actors can be blocked, even when against the will of European governments[150].

The European Commission is in favour of market-based pan-European payment solutions such as the European Payment Initiative (EPI). In 2019, EPI was founded with the political support from the European Commission[151] and the European Central Bank[152]. While its initial goal was to have a pan-European card payment scheme up and running by the second half of 2022, that goal has recently been adjusted. Of the initial 31 banks and acquirers, just 13 remain, and they are said to be refocusing on launching a digital wallet, instead of a full-blown card scheme[153]. An update is expected regarding the exact adjustment of scope from the EPI but was not available at the time of writing this report.

When completed, the pan-European payment solution by the European Payment Initiative will affect the following needs:

149 https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2764
150 Conclusion 7: https://data.consilium.europa.eu/doc/document/ST-6301-2022-INIT/en/pdf
151 https://ec.europa.eu/info/news/200702-european-payments-initiative_en
152 https://www.ecb.europa.eu/press/pr/date/2020/html/ecb.pr200702~214c52c76b.en.html
153 https://thepaypers.com/payments-general/epi-adapts-its-scope-and-objectives-as-member-banks-withdraw--1255282

- First, the **need to resolve the fragmented market for innovative payment solutions** would become slightly less relevant. The creation of a pan-European payment solution, be it in the form of a card network or a digital wallet is likely to ease cross-border innovative payments. Innovative payment solutions can build their propositions around this pan-European payment solution and as a result scale more easily across the European Union. The market for innovative payment solutions would become less fragmented as a result.
- Second, the **need for more effective competition in certain payment areas** would become slightly less relevant as a widely accepted and used pan-European payment solution would compete with the established international card schemes (Visa and Mastercard). As the number of competitors increases, competition is expected to become more effective and hence the relevance of this need reduced.
- Third, the **need to strengthen the resilience and autonomy of the European payments sector** would become less relevant. A homegrown, pan-European payment solution would reduce the dependency of the European payments market on foreign financial infrastructure and thus strengthen the autonomy and resilience of the European payments market.

Policy development 3: The push for implementation and adoption of instant payments

Instant payments are payments completed in the span of seconds, 24 hours a day, seven days a week. An instant payment enables both customers and merchants to directly confirm transfers and have the funds available immediately. As a result, the billions of euros that are otherwise in transit are available at once for consumption and investment. Lastly, instant payments based on SEPA instant have pan-European reach and would contribute to the Commission's objective of increasing the autonomy of EU payment solutions.

Since the introduction of PSD2 the implementation of pan-European instant payments has continued, for example with the introduction of the TARGET Instant Payment Settlement market infrastructure. However, the actual number of payments completed through instant payments have lagged, standing at 7% of total payments in the first half of 2020[154]. In its Retail Payment Strategy from 2020, the European Commission has therefore restated its intentions, expressing its ambition for instant payments to become the 'new normal'[155].

The adoption of instant payments, once fully materialised, will affected the following needs:

- First, the **need for more effective competition in certain payment areas** becomes less relevant would be impacted by the rise of instant payments, which are based on SEPA Instant, which is a form of account-to-account based payments. SEPA Instant can be used by established players and new entrants alike, without a difference in its capabilities, creating a level playing field. It also requires fewer parties in the payment processing chain, and generally comes with a low cost as a result. Instant payments, once fully adopted, are therefore expect to improve the level playing field and stimulate price competition, making the need for more effective competition less relevant.
- Second, the **need to resolve the fragmented market for innovative payment solutions** would become less relevant as SEPA Instant is designed as a pan-European solution, and therefore does not face the cross-border interoperability issues that might plague other solutions (such as the domestic account-to-account schemes discussed earlier).
- Third, the **need to strengthen the resilience and autonomy of the European payments sector** would become less relevant. A full adoption of instant payments would decrease the reliance on foreign financial infrastructure (for example, that of non-European international card schemes) and thus boost the autonomy and resilience of

[154] https://www.ecb.europa.eu/paym/intro/mip-online/2020/html/2011_mip_online.en.html
[155] Retail Payment Strategy, Pillar 1

the European payments sector. The need to strengthen it will therefore become less relevant.

Conclusion

The following section concludes the analysis of developments and policy developments since the adoption of PSD2 on the needs. The results are summarised in Table 6 and Figure 11. When evaluating the relevance of the needs along the lines of (1) current market developments, (2) new market developments and (3) political developments, the following results are found:

- Continuing market developments affirm the relevance of various initial needs. In particular, the relevance of more effective competition is affirmed. For example, by barriers to entry resulting in the limited market penetration of innovative payment solutions and the fragmentation of payments markets. The latter development naturally also affects the relevance of reducing the fragmentation of payments markets.
- The relevance of the need to harmonise licensing and supervisory practices, and of a consistent application of PSD2, are similarly affirmed by continuing market developments. Specifically by the development that shows divergence in application and supervisory practices of PSD2. Lastly, the relevance of increased consumer protection is affirmed as a result of continuing market developments in the fields of fraud and contactless payments.
- New market developments affirm the need of regulating the status of all payment providers and more effective competition – e.g., through the emergence of premium APIs and API aggregators. The relevance of increased consumer protection is also affirmed by those two developments. Other needs affected by new market developments are the new need to strengthen the autonomy and resilience of the European payments market as well as the need for less fragmentation of payments markets. The first is affected by the rise of BigTechs, whereas the latter is affected by the growth in account-to-account payments. The relevance of both needs is increased as a result of these developments.
- Policy developments have the potential to affect the relevance of more competition, less fragmentation of payments markets and a more autonomous and resilient European payments market. Contingent on their successful pursuit, of course, as their actual effect remains uncertain. Potentially most impactful are the policy developments surrounding a pan-European payment solution and the adoption of instant payments. These developments have the potential to increase competition, reduce fragmentation, and strengthen the autonomy and resilience of the European payments market. They could thus reduce the relevance of the aforementioned three needs.

Figure 11: Visualisation of developments' impact on needs

Note: Relevance levels are only an indication, no direct result of adding and subtracting developments, and based on policy and future developments whose outcome remains uncertain.
Source: VVA and CEPS analysis (2022).

The only need unaffected by continuing, new or policy developments is the need to harmonise charging and steering practices between Member States. This need loses some of its relevance as a result of the surcharging ban. The surcharging ban has harmonised charging and steering practices for a large share of payments in the EU. Yet not all types of payments are covered by it, and some divergence still exists as a result. For example, in the Netherlands and Germany surcharging is allowed for three-party card schemes, whereas in neighbouring Belgium it is not[156]. Seeing that 95% of card payments are subject to the surcharging ban, national divergences affect only a very small part of the payment market[157]. In the rare occasion

[156] See Table 1: https://cmspi.com/eur/en/resources/content/psd2-the-european-payments-revolution-part-3-surcharging/
[157] https://ec.europa.eu/commission/presscorner/detail/de/MEMO_13_719

that surcharges are applied in a Member State, the surcharge is no longer allowed to surpass the actual cost the merchant incurs for accepting the payment (i.e. surcharging to increase revenues is illegal). Seeing that charging and steering practices are harmonised across Member States to a large extent, and that when a surcharge is applied it is capped at the actual cost the merchant incurs, the need to harmonise charging and steering practices across countries is reduced.

Table 6: Overview of market- and policy developments' impact on the relevance of needs

Needs	Continuing market developments						New market developments							Policy developments		
	1: Fragmentation of the payment services market	2: Market penetration by innovative payment solutions	3: Ineffective competition in certain areas of internet payments	4: Diverging licensing and supervisory practices	5: Increasing use of cashless and contactless payments	6: Diverging fraud rates and emergence of new types of fraud	1: Emergence of premium APIs	2: Emergence of API Aggregators	3: Emergence of 'license-as-a-service' providers	4: Entry of BigTechs to the payments market	5: Growth in account-to-account payment services	6: Growth of digital wallet services	7: The rise of buy-now-pay-later services	1: Opening restricted technical infrastructure	2: The push for a pan-European payment solution	3: The push for implementation and adaptation of instant payments
1: Regulating the status of all payments service providers							++	++	++	+	+	++				
2: More effective competition in certain payment areas	+	++	+				+	++	++	++	+	+		-	-	-
3: Fragmented market for innovative payment solutions	++				+						+				-	-
4: Harmonisation of licensing and supervisory rules and practices				++												
5: More consistency in the application of PSD				+												
6: Harmonisation of charging practices between member states																
7: Increased consumer protection					+	+	+	+	+				+			
New: Strengthen the autonomy and resilience of the European payments market										+					-	-

Note: The "++", "+", "+-" and "-" signify how the development affects the need. A ++ means a strong positive impact, a + means a moderate positive impact, a +- means both a positive and negative impact, and lastly a - means a negative impact.Source: VVA and CEPS analysis (2022)

5.1.2. How are the needs expected to evolve in the future?

In future, it is very likely that without further policy interventions the market developments discussed in the previous sections will continue. In addition, there are a number of potential future developments that could have an impact on relevance.

This section discusses the impact of those developments on the needs to be addressed by the PSD. It is based on interviews as well as analysis of industry publications and policy documents.

The following major market developments might occur in the future and affect the needs of PSD2:

1) Introduction of a digital euro;
2) Use of crypto-assets as a means of payment;
3) Furthering payment initiation services;
4) Unification of POS and online payments in commerce; and
5) Further shift of commerce to digital marketplaces and platforms.

The section discusses each of these major potential future market developments and analyses how it they would affect the needs to be addressed by the PSD2.

Future development 1: Introduction of a digital euro

The ECB is exploring the issuance of a Central Bank Digital Currency (CBDC), a currency that is digital by nature and would complement the euro in its current form (cash)[158].

A declining usage of cash, an increasingly digital economy and the rise of cryptocurrencies have spurred central banks to explore the option of issuing a digital currency. Currently, a large number of central banks are studying the possibility of issuing a CBDC. Some have already introduced (in pilot form) a CBDC (digital Yuan, People's Bank of China) or are on the cusp of doing so (digital Rupee, Reserve Bank of India)[159].

While the design of the ECB-issued CBDC is still being studied, officials have signalled that the digital currency is expected to facilitate resilient, fast and inexpensive payments. In addition, it is expected to facilitate new forms of payments, such as automated and conditional payments[160]. Lastly, it has the potential to reduce reliance on international card schemes for facilitating payments and provide a viable alternative to competing, not central bank backed, (crypto) currencies[161]. The latter two effects will benefit the EU's financial autonomy.

The ECB-issued CBDC has the potential to affect the needs of PSD2 in many ways. Focusing on technical advancements that the CBDC will bring resilient, fast and low-cost (potentially free) payments, we can expect the following needs to be affected in particular:

- First, the **need for more effective competition in certain payment areas** is expected to lose relevance. A CBDC will be a fast and cheap alternative to current payment methods, invigorating competition. In addition, it can be the backbone on which new innovative payment solutions are created, which can then leverage its pan-European reach to easily scale across the European Union. This would provide another boost to competition in the payments market. As competition in certain payment areas is therefore expected to increase following the introduction of a CBDC, the need for more effective competition is reduced..
- Second, the **need to resolve the fragmented market for innovative payment solutions** is affected as the CBDC is expected to function by the same technological standards across the eurozone. As a result, innovative payment solutions that rely on

158 https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210714~d99198ea23.en.html
159 https://www.atlanticcouncil.org/cbdctracker/
160 https://www.ecb.europa.eu/press/key/date/2021/html/ecb.sp211105~08781cb638.en.html
161 https://www.ecb.europa.eu/press/key/date/2021/html/ecb.sp211118~b36013b7c5.en.html

the CBDC are not expected to be restricted by regulatory divergences across Member States. Even when an innovative solution is initially designed for just one Member State it should easily scale to the eurozone as a whole. The relevance of the need is thus reduced.

- Third, the **need to strengthen the autonomy and resilience of the European payments market** is expected to reduce in relevance. An ECB-issued CBDC will be a homegrown payment solution that is expected to function on European financial infrastructure. Therefore, assuming that the ECB-issued CBDC will become a widely adapted means of payment, the dependency on foreign financial infrastructure will reduce. Consequently, the need to strengthen the autonomy and resilience of the European payments market will reduce as well.

Future development 2: Use of crypto-assets as a means of payment

Crypto-assets and their service providers have remained unregulated in nearly all Member States since the introduction of Bitcoin in 2009. However, recently regulators have taken greater attention to developments in the field of crypto-assets, to both reap the potential benefits and reduce the risks of crypto-assets.

In Europe, the most prominent example of a regulatory initiative on crypto-assets is the Markets in Crypto-Assets (MiCA) Regulation[162]. Having recently passed "trilogue" negotiations, the MiCA Regulation sheds light on how crypto-assets and their service providers are likely to be regulated in the future. Relating to PSD2, the Regulation sheds light on the role of crypto-assets as a means of payment and their role in the payments market.

MiCA and similar regulatory initiatives originate from a need to regulate crypto-assets so as to avoid them becoming (too big of) a threat to financial stability and to put consumer protections in place. Crypto-assets can become a threat to financial stability when they become an unregulated, widely accepted means of payment, as well as when they become interconnected with the traditional financial system, while retaining their volatile nature. Recent publications of the FSB highlight those threats, while the recent crash and demise of some so-called stablecoins displays the volatility and risks currently associated with crypto-assets[163].

The legal framework laid out in MiCA helps mitigate the aforementioned risks of crypto-assets. Specifically, it does so by classifying types of crypto-assets and tailoring the regulation to these categories. For the payments market, the crypto-assets falling within the categories of "asset-referenced tokens" and "e-money tokens" are of relevance, seeing that they in effect are (partial) money substitutes, as noted by the ECB in their opinion on MiCA Regulation[164].

Keeping in mind the uncertainty about the exact implementation and consequences of MiCA, if we assume asset-referenced tokens and e-money tokens to become (partial) money substitutes, the following needs of PSD2 are expected to be affected by the adoption of crypto-assets as a means of payment:

- First, the **need for more effective competition in certain payment areas** could be enhanced since asset-referenced tokens and e-money tokens will compete with established means of payment and benefit from their digital-first nature; they can reinvigorate competition across payment methods in order for non-crypto based payment methods to stay competitive.
- Second, the **need to resolve the fragmented market for innovative payment solutions** is reduced as the regulation of crypto-assets provides a boon for innovative payment solutions in general, and by allowing them to create propositions around the use of asset-referenced tokens and e-money tokens. Furthermore, it reduces the fragmentation of payment solutions seeing that the MiCA Regulation concerns the EU,

[162] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0593&from=EN
[163] https://www.fsb.org/2022/02/assessment-of-risks-to-financial-stability-from-crypto-assets/
[164] Point 1.2: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021AB0004&from=EN

and propositions revolving around asset-referenced tokens and e-money tokens should therefore easily scale across the EU.

- Third, the **need for increased consumer protection** is expected to remain relevant. Consumers are generally ill-informed about the risks and opportunities related to crypto-assets because of their highly technical nature and the rapid development of the crypto-asset market[165]. Moreover, crypto-asset markets have proven themselves to be highly volatile and prone to speculating, two trends that generally do not benefit consumers. While wider acceptance of crypto-assets as a means of payment and the maturation of the crypto-asset market may improve consumer knowledge on crypto-assets and reduce the volatility and speculation currently witnessed in the crypto-asset market, the need for consumer protection is for now expected to remain relevant.

Future development 3: Furthering payment initiation services

Alongside account information services, PIS is one of the new services that PSD2 enabled. While account-to-account payments, which PIS facilitates, have grown since the introduction of PSD2, this growth followed mostly from domestic initiatives through which the major banks in a country facilitated fast and low-cost account-to-account payments among themselves[166]. PIS, as envisioned in PSD2, go beyond these domestic initiatives, and their use is therefore expected to increase.

PIS as enabled by PSD2 is an improvement over current payment methods since it (1) allows for cross-border payments, (2) provide both parties with fast confirmation on the completion of the transaction, and (3) are designed to be low cost. The benefits materialise especially on the side of merchants, as PSD2-enabled PIS allows them to speedily receive funds at a low cost for customers all over the EU[167].

Given the vast benefits of PSD2-enabled PIS, the use is expected to increase. However, the use of PSD2-enabled PIS has been lagging, illustrated by figures by some industry participants that less than one in ten API calls is for PIS, and that few to no concrete use cases are currently found[168].

This lack in uptake is seemingly explained by (1) established domestically operated alternatives such as Sofort and iDeal, (2) the prohibition on surcharging and (3) APIs/obstacles to use TPPs at POS. Without a surcharge, merchants have limited possibilities to incentivise customers to use the cheaper payment methods. They have the possibility to give rebates, but this is not used much. Domestic alternatives for account-to-account payments are therefore hard to compete with, especially given their familiarity to customers and similarly low costs and speedy transfers. As such, there are at present few concrete benefits to customers to using PSD2-enabled PIS, and a downside is presented in the form of having to acquaint oneself with a new type of payment service and giving consent.

While the extent to which PISs' potential will materialise remains uncertain, the following needs are expected to be affected when PISs realise their potential as an established, widely used, payment method:

- First, the **need for more effective competition in certain payment areas** is reduced enhanced as PSD2-enabled PIS provide a highly competitive alternative to established methods of payment, and one that in theory should be easy to adapt for merchants and consumers alike.
- Second, the **need to resolve the fragmented market for innovative payment solutions** is reduced as PSD2-enabled PIS are cross border by design. Innovative

165 https://www.fca.org.uk/publications/research/research-note-cryptoasset-consumer-research-2021
166 IDeal, Giropay and Swift are examples of such domestic initiatives
167 In a recent survey among financial executives, these benefits in addition to higher security were identified as the primary benefits of PISs for merchants: https://tink.com/blog/open-banking/report-future-of-payments-open/
168 API Aggregator Ibanity reports that over 90% of its API calls are AIS calls, a similar number to what was reported by another party during an interview. https://ibanity.com/blog/the-challenge-of-monetizing-psd2.

payment solutions based on them will therefore not be restricted by national borders, and the fragmentation of innovative payment solutions along national borders should thus decrease.

Future development 4: Unification of POS and online payments in commerce

Many retailers already operate under a so-called 'omnichannel' business model, i.e. serving customers through multiple channels such as a combination of a web shop and retail storefront. The next step in integrating and expanding the retail experience for customers is 'unified commerce', which connects the various channels of a retailer and makes sure both payment methods as well as data collection are synchronised within the limits of the data protection rules. As a result, merchants have a richer set of data on customer behaviour and sales to draw insights from, while customers enjoy a smoother shopping experience across channels.

In practice, unified commerce facilitates shifts in payments behaviour that are likely to benefit digital payment methods. For example, at a retailer with a unified commerce system in place, the consumer may order and pay for goods on its way to the shop, only to pick them up there. Or after browsing and having found a product to be purchased, the consumer may pay for it on the spot through the web shop of the retailer. Unified commerce therefore enhances the flexibility a consumer has in paying for goods or services and breaks down the separation between e-commerce and POS payments. Since the expansion of payment methods is tilted towards digital ones – one can after all only pay with cash in a physical location – digital payment methods, including e-wallets, are expected to benefit from this switch.

As unified commerce solutions gain ground, the following need is expected to be affected:

- The **need for more effective competition in certain payment areas** is affected as unified commerce has the potential to both increase and decrease competition in certain payment areas. On the one hand, providing a comprehensive solution that covers both payment methods and data analysis across sales channels creates a lock-in effect. Merchants may want to prefer the payment services offered by a different provider but find themselves bound to the data analysis platform of their current provider, reducing their flexibility in switching providers and thus the potential for competition.
- On the other hand, the choice of payment methods available to consumers is expected to increase, as a consumer can choose its preferred method of payment across channels, being no longer restricted to paying at a counter, for example. As payment service providers can easily offer a wide array of (digital) payment methods, competition across these methods, and for traditional card schemes, is expected to increase. The move towards unified commerce affects competition in certain payment areas and is therefore a double-edged sword: competition among payment methods is expected to increase, whereas that among payment service providers may decrease.

Future development 5: Further shift of commerce to digital marketplaces and platforms

Digital marketplaces, such as eBay or Etsy, have been around since the early days of the internet. In recent years, they have vastly expanded as new digital marketplaces and platforms are created for goods and services previously only distributed via traditional channels[169]. This development is expected to continue in future.

Concrete examples of new forms of digital marketplaces include:

- A local farmers market creating an online marketplace where consumers can shop for products from a variety of distributors and pay for those goods in a single payment; and
- A marketplace where a certain group of professionals, say illustrators, offer their services and are contracted and paid through the digital marketplace.

[169] In its 2021 Global Payment Report, consultancy firm McKinsey states its expectation that 50 to 70 percent of digital commerce will be conducted on digital marketplaces and platforms:

Beyond offering an online distribution channel, digital marketplaces also offer different payment methods and may offer accounting and data analytics to the merchants using the marketplace.

As these marketplaces are usually serviced by a single PSP which is responsible for all payments done on the platform, a shift of commercial activity towards digital markets also carries significant implications for how payments are made. As a result, the position of PSPs is more likely to become entrenched, while the number of payment methods offered is much easier and more likely to be expanded.

The following needs are affected as a result of the shift of commerce to digital marketplaces:

- The **need for more effective competition in certain payment areas** is affected as the shift of commerce towards digital marketplaces has the potential to increase and decrease the competition in certain payment areas. As with unified commerce, the servicing of the entire marketplace by a single payment provider means that lock-in effects exist and that marketplaces do not easily switch between payment service providers. The market for payment service providers may therefore become more consolidated and less competitive as a result. Yet, at the same time, the facilitating of payments through a payment service provider, instead of having every merchant choose a method (or methods) of payment itself, means that the number of payment methods offered is likely to be much greater, and is more easily expanded or changed. This will benefit the competition among payment methods as new methods are more easily offered and can more effectively compete against incumbent methods.

Conclusion

The following section concludes the identification of potential future developments and their likely impact on the relevance of needs underpinning PSD2. The main findings are summarised in Table 7.

The effect of future developments on future needs is uncertain by nature. Yet if and when they materialise, they can impact on relevance. For example, if a digital euro is introduced or if crypto-assets become a common form of payment, this might increase competition and reduce fragmentation of the payments market, thus reducing the relevance of the corresponding needs.

The relevance of increased consumer protection as well as that of a more autonomous and resilient European payment market are also likely to be affected if future developments become reality. The relevance of increased consumer protection could increase if crypto-assets become a common form of payment – e.g., because of the volatility of crypto-assets. The need for the PSD to foster an autonomous and resilient European payment market could reduce when a digital euro is introduced because it would be a payment based on homegrown financial infrastructure.

Overall, potential future market developments are expected to improve the competitiveness and autonomy of the European payments market. These future market developments have the potential to reinvigorate competition in the payments market and push the development of pan-European payment solutions.

Table 7: Overview of potential future developments' impact on the relevance of needs

Needs	Future developments				
	1: Introduction of a digital Euro	2: Use of crypto-assets as a means of payment	3: Furthering payment initiation services	4: Unification of POS and online payments in commerce	5: Further shift of commerce to digital marketplaces and platforms
1: Regulating the status of all payments service providers					
2: More effective competition in certain payment areas	-	-	-	+-	+-
3: Fragmented market for innovative payment solutions	-	-	-		
4: Harmonisation of licensing and supervisory rules and practices					
5: More consistency in the application of PSD					
6: Harmonisation of charging practices between member states					
7: Increased consumer protection		+			
New: Strengthen the autonomy and resilience of the European payments market	-				

Note: The "++", "+", "+-" and "-" signify how the development affects the need. A ++ means a strong positive impact, a + means a moderate positive impact, a +- means both a positive and negative impact, and lastly a - means a negative impact.
Source: VVA and CEPS analysis (2022)

5.1.3. To which extent does PSD2 address current developments in the field of payment services?

PSD2 addresses current developments in the field of payment services to a large extent. Current developments can be split in two: those that originated before and after PSD2. Current developments that originated before are discussed in the continuing market developments sections. In this section, the objectives underpinning PSD2 are shown to apply to the relevant needs based on continuing market developments.

Current developments that initiated after PSD2 are discussed in the new market developments section above. Although PSD2's objectives were not designed with these developments in mind, new market developments are also well covered by the current objectives. The inclusion of a new need for a more autonomous and resilient European payments market would improve the extent to which PSD2 addresses new policy priorities[170].

The need and accompanying objective addressing the divergence of charging and steering practices across Member States has become less relevant as the divergence in charging and steering practices has reduced since the introduction of PSD2. Nevertheless, Member States are still permitted some discretion in applying exemptions from the surcharging ban. Thus, if there is a need to further harmonise steering and charging practices across countries, it must be designed with this development in mind.

Seeing that a vast majority of current developments is addressed in the needs by PSD2, it is concluded that PSD2 addresses current developments in the field of payments to a large extent.

[170] Especially the policy development concerning the "push for a pan-European payment solution"

General and specific objectives

To further assess the extent to which PSD2 addresses current developments in the field of payment services, the relevance of the general and specific objectives of PSD2 is assessed. Objectives are considered relevant if they continue to address the need to which they are linked, even when that need has evolved. New needs can also emerge due to the change in financial market conditions. The general and specific objectives are summarised in Figure 12.

As the figure shows, the following general and specific objectives were set up with PSD2:

1) Ensuring a level playing field between incumbent and new providers of internet and mobile payments (general objective 1), and ensuring that emerging payment service providers are covered by the regulatory framework governing retail payments in the EU (specific objective 1);
2) Addressing competition issues (specific objective 2);
3) Facilitating the provision of internet and mobile payment services across borders (general objective 2), and addressing standardisation and interoperability issues for online and mobile payments (specific objective 3);
4) Creating an environment which helps innovative payment services (general objective 3);
5) Better aligning charging and steering practices for payments services across the EU (specific objective 4);
6) Increasing the efficiency, transparency and choice of payment instruments for users (general objective 4), and improving the consistent application of PSD across Member States and better aligning licensing and supervisory rules (specific objective 5); and
7) Ensuring a high-level protection for users across all member states of the EU (general objective 5), and protecting consumer interest and extending protection to new channels and innovative payment services (specific objective 6).

Below the relevance of each of the objectives is discussed in more detail.

General objective 1: Ensuring a level playing field between incumbent and new providers of internet and mobile payments and Specific objective 1: Ensuring that emerging payment service providers are covered by the regulatory framework governing retail payments in the EU

The need to regulate the status of all payment service providers (need 1) is covered by the general objective to ensure a level playing field between incumbent and new providers and by the specific objective of ensuring that emerging payment service providers are covered by the regulatory framework governing retail payments in the EU.

An emerging payment service is the premium API. ASPSPs offering premium API services, give actors that would like to enter the market and offer AIS or PIS the possibility to offer their customers services that go beyond what is defined under PSD2. The requirements premium API users must follow are interpreted differently, with in some cases unlicensed TPPs gaining access to the similar information as through the APIs licensed under PSD2.

In addition, there are new market actors acting as API aggregators or offering licence-as-a-service that risk giving certain TPPs a potentially unfair advantage compared to incumbents. API aggregators offering the licence-as-a-service make it possible for TPPs that do not hold a PSD2 licence to offer AISs and PISs to their customers.

Based on the previous needs and market developments, the specific objective of ensuring that new market actors fall under the same regulatory framework, and the general objective to ensure a level playing field are therefore still considered relevant.

Specific objective 2: Addressing competition issues

The need for more effective competition in certain payment areas (need 2) is linked to the specific objective of addressing competition distortions. There are still discrepancies in the level playing field for card payments and digital payments. Additionally, digital wallets have also entered the payments market, which can be offered without a PSD2 licence and generates

additional costs for ASPSPs. Different payment methods facing varying requirements indicate that the objective of addressing competition issues remains relevant.

General objective 2: Facilitating the provision of internet and mobile payment services across borders and Specific objective 3: Addressing standardisation and interoperability issues for online and mobile payments

In order to address the need for a more integrated market for innovative payment solutions (need 3) there are two accompanying objectives: (a) the general objective to facilitate the provision of internet and mobile payments across borders; and (b) the accompanying specific objective of addressing standardisation and interoperability issues for online and mobile payments.

Digital payment solutions are still fragmented between markets, with limited ability to perform cross-border payments. What can be observed is the development of initiatives is an attempt to stimulate cross-border interoperability, such as the initiative for the standardisation and interoperability of the European Payments Council's QR-code of SEPA credit transfers initiated via mobile[171]. However, with the persistent fragmentation and limited cross-border interoperability[172], both objectives remain relevant.

General objective 3: Creating an environment which helps innovative payment services

The need to harmonise the licensing and supervisory rules (need 4) is addressed by the objective to create an environment that helps innovative payment services. Both licensing and supervisory practices have diverged between Member States since the launch of PSD2. This fragmentation across markets has led to innovative payment solutions developed by TPPs struggling to gain traction, and traditional payment methods such as card or cash remaining dominant. Thus, the general objective to help innovative payment services remains relevant.

Specific objective 4: Better alignment of charging and practices for payment services across the EU

A need that was identified during the preparation of PSD2, was the harmonisation of charging practices between Member States (need 5), which was addressed by the specific objective for better alignment of charging and practices for payment services across the EU. This objective has lost relevance. The ban on surcharges harmonised charges across markets, steering practices in a common direction, partially or fully reaching the intended target of harmonising charging practices between Member States. Therefore, the objective is of limited relevance today as there is no longer a need for alignment of charging practices.

General objective 4: Increasing the efficiency, transparency and choice of payment instruments for users and Specific objective 5: Improving the consistent application of PSD across Member States and better aligning licensing and supervisory rules

The need for more consistent application of PSD2 (need 6) has the accompanying general objective of increasing efficiency, transparency and choice of payment instruments for users, and the specific objective of improving the consistent application of PSD2 across Member States and better aligning licensing and supervisory rules. Access to clear guidance and responses to regulatory questions from national supervisors vary between Member States resulting in interpretational and market transparency issues for new market actors, incumbents and users.

For new entrants there are also diverging licensing processes with varying times between requesting a licence and receiving a response across Member States. This limits the possibility for interested parties to enter the market. With diverging guidance and implementation of the Directive across Member States[173] these objectives remain relevant.

[171] www.europeanpaymentscouncil.eu/news-insights/news/final-version-standardisation-qr-codes-mscts
[172] See also the Continuing market developments section
[173] See also the Continuing market developments section

General objective 5: Ensuring a high-level protection for users across all Member States of the EU and Specific objective 6: Protecting consumer interest and extending protection to new channels and innovative payment services

The need to increase consumer protection (need 7) has the accompanying general objective of ensuring a high level of protection for users across all Member States. Additionally, there is an underlying specific objective of protecting consumer interests and extending protection to new channels and innovative payment services. The development of new market actors acting as API aggregators or offering licence-as-a-service has added a potential additional middleman in the flow for access to payment services. This has made it more complicated for the ASPSP to identify who is accessing a customer's account, and what party is initiating a payment or accessing consumer data.

The increased use of digital payments has led to new security risks for online payments. Authentication methods have been developed in order to counter this risk, but they are not harmonised. With the new services sometimes falling outside of the scope of PSD2 and the unharmonised authentication methods to access account information, both objectives remain relevant.

Needs not covered by current objectives

The new need to strengthen the autonomy and resilience of the European payments market (need 8) is not directly addressed by the current set of objectives. While the fulfilment of some objectives, such as the objective for increased interoperability and standardisation, or the objective for less fragmentation of payment services, will partially address the new need, it is not covered comprehensively.

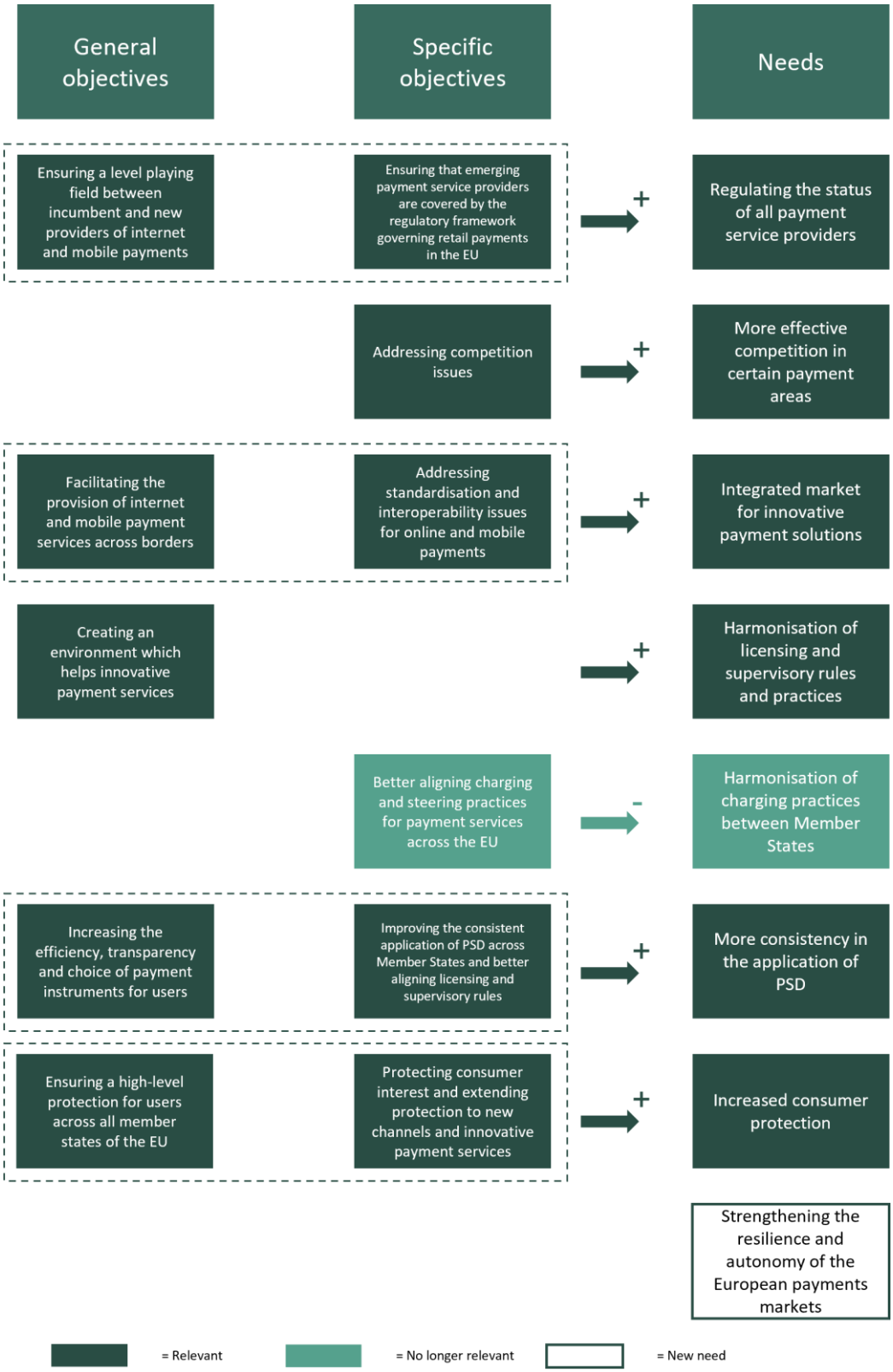
In order to directly address the need for a more autonomous and resilient European payments markets new objectives must be formulated. Such objectives would target a shift of European payments towards homegrown financial infrastructure, aim to diversify the reliance on foreign technical infrastructure and promote European payments schemes. Examples of such objectives could be (1) the creation of a pan-European payment solution, (2) guarding against the market power of BigTech in the payments market, and (3) the promotion of implementation and adoption of European payment schemes such as SEPA Instant.

Conclusion

The objectives of PSD2 continue to a large extent to address the current needs. The exception is the objective on steering charging practices across countries which has become less relevant as it has to a large extent been achieved. Also, when a new need covered by current objectives to strengthen the autonomy and resilience of the European payments market would be introduced accompanying objectives will have to be formulated.

Figure 12 provides a condensed overview of the different general and specific objectives of PSD2 and the needs guiding these objectives.

Figure 12: Overview of General and Specific objectives' relevance



Source: VVA and CEPS analysis (2022)

5.2. Effectiveness

Effectiveness assesses the extent to which the PSD2 has achieved its objectives. This chapter therefore analyses the impact of the legislation in terms of whether it has led to economic benefits for payment service providers and payment service users; if there have been challenges encountered in the market as a result of the legislation; whether it has meant higher protection for PSUs; whether it has enhanced cross-border payments; the extent to which the legislation has helped TPPs access accounts; and whether there are issues in enforcing measures stipulated by PSD2. This section also assesses the effectiveness of the definitions in the PSD2, the licensing regime for payment institutions, the superversion of PSPs, the transparency of conditions and information requirements, SCA requirements and the rights and obligations of market actors.

Overall, the chapter finds that there has been progress in meeting the goals of the PSD2 though issues in implementation have meant these goals have not been fully met and market actors have faced some difficulties in operating in the new legislative environment. In the case of open banking, legislation has allowed for structured interaction between ASPSPs and TPPs for AIS and PIS but ASPSPs are concerned about the costs they incur due to the free access they are required to provide, and the latter argue their access is consistently hindered. Similarly, when it comes to supervision, there is agreement that oversight has increased as a result of the Directive but supervisors have not been able to address key issues raised by both TPPs and ASPSPs effectively and efficiently, which in turn has hampered their ability to provide services in line with the expectations of PSD2. Another key finding is that several aspects of PSD2 have seen unharmonised implementation among Member States which has created difficulties for entities seeking to provide services across borders. Finally, stakeholders frequently agree that the intention behind some of PSD2's measures are appropriate but that they can lead to disproportionate requirements on PSPs, such as in transparency requirements, licensing regimes and SCA.

Evidence gathered for this section is based on the literature review and, primarily, the stakeholder consultation performed as part of this evaluation. The extent to which stakeholders had perspectives on the evaluation questions detailed below differed greatly across the topics. Extensive experience and knowledge was demonstrated for example for questions concerning access to accounts, but less so as regards for example transparency of conditions and information requirements.

This section seeks to answer the following evaluation questions:

- What has been the impact of PSD2?
- How does the impact relate to the objectives of PSD2?
- To what extent does the scope of PSD2 drive or impede achievement of its objectives and impact?
- To what extent does the clarity of definitions within the PSD2 drive or impede achievement of its objectives and impact?
- To what extent does the PSD2 licensing regime drive or impede achievement of its objectives and impact?
- To what extent does the supervisory framework within the PSD2 drive or impede achievement of its objectives and impact?
- To what extent do transparency of conditions and information requirements drive or impede achievement of its objectives and impact?
- What has been the impact of strong customer authentication (SCA)?
- What has been the impact of rights and obligations (e.g., regarding charges, liability and recovery of damages)?
- What has been the impact of data access and data sharing rules?

5.2.1. The impact of PSD2

This section describes the economic (and non-economic) benefits and the drawbacks brought about by PSD2 by analysing the impacts on payment service providers and users. This section also sheds light on a number of issues and challenges in the enforcement of PSD2.

Overall, there is an agreement that, compared to previous legislation, PSD2 has brought about important benefits but specific issues remain. This overall result is also confirmed by the survey which shows a mixed picture regarding the impact of the PSD2.

Main benefits brought by PSD2

The study findings indicate that PSD2 has allowed for greater competition as new businesses and business models have entered the market. This has also fostered innovation. Furthermore, open banking provisions has meant that TPPs have been able to access data through regulated APIs rather than screen scraping. Furthermore, it has permitted market actors to provide services across the EU through the passporting regime. Stakeholders participating in the interviews and answering survey questionnaires highlighted key benefits brought by PSD2, namely, the fact that PSD2 enabled a flourishing ecosystem of payment service providers laying the conditions for user-friendly, accessible, transparent, innovative and secure payments for European businesses and citizens, supporting the needs of merchants and citizens in the online economy. Nonetheless, market participants also highlight issues that have prevented them from obtaining these benefits to the fullest extent (these are discussed in subsequent sections).

There is consensus across a wide spectrum of stakeholders that the PSD2 has been a major step forward for the payments industry by enabling the emergence of new business models. Like its predecessor PSD1, PSD2 has facilitated market access for non-bank payment providers. The ability for payment service providers to access a Single Market for payments in the EU, and to passport their licence across that market was a significant factor for the development of the payments market in Europe: PSD2 has therefore had an overall positive impact on competition. Furthermore, considering the wider ecosystem, national supervisors have indicated that PSD2 created a clearer market structure and predictability on the market by regulating previously unregulated actors and services. These stakeholders considered that an important aspect of this involved the establishing of security requirements for the interaction of ASPSPs with TPPs.

The provisions on access to payment data are enabling innovative solutions to be developed, providing more choice to consumers in the way they pay online. These solutions, widely described in chapter 3, are based on the sharing of payment account data such as payment initiation services (PIS) and account information services (AIS). Several ministries noted that there was previously a market for payment initiation and account information services under PSD1 but since the implementation of PSD2, there has been a significant growth in the market for such services. Several ministries indicated that they have received more licensing applications in the area of AISPs and PISPs. One interviewee noted that in their Member State of jurisdiction, there has been a growing number of such institutions (around 100 within the market). Similarly, a national supervisor in another Member State pointed out that before PSD2 there were roughly 10-12 payment institutions and AISPs, compared to over 40 nowadays. Notably, these services are still very much in their infancy and this supervisor is observing more and more firms on the market developing new products and services. PISPs have also indicated that PSD2 has enabled their business models to function as there is now the possibility for them to initiate payments.

The PSD2 has led to the entry of new market players which created additional competition for banks. BigTech firms, such as Google, Amazon and Facebook would have the possibility to further integrate their interaction with customers and could in theory compete with banks on payments, if they became licensed PSPs by offering integrated payment options. Like banks, the BigTech firms have multiple revenue streams giving them the possibility to

develop very competitive business models (Oliver Wyman, 2016). On the other hand, if BigTechs are able to leverage network effects (i.e. having already access to many users and their data) this may provide them with an advantage over other players in the market, which could undermine competition in the longer term.

As observed by a national ministry and a consumer association, alongside enabling entry in the payments market, PSD2 also triggered innovation in incumbents' legacy business models. For example, the emergence of e-money firms offering instant payments pushed traditional banks to move into the instant payment space[174]: according to this interviewee, this would not have happened without PSD2. It should be noted, however, that one PSP has indicated that while there has been an influx of new businesses, they are not always sustainable as many soon after exit the market. Another instance of innovation, mentioned by a credit bureau, can be seen as a result of open banking provisions in PSD2 which have meant APIs can provide much richer sources of data when compared to the previous regulatory context in which screen scraping was used. Open banking requirements (access to payment accounts data), unlocked the possibility to combine analytics and machine learning techniques to understand payment patterns and derive some KPIs with bank data. Together with the regulatory developments, as noted by a PSP, it is worth noting the role played by the pandemic as a further innovative driver: this unexpected factor raised customers' sensibility and appetite for digitalisation of payment processes, facilitating a better understanding of the opportunities offered by the PSD2. In fact, this PSP observed that right now an acceleration in the request of open banking-based services is visible.

Moreover, PSD2 provided the legislative and regulatory foundations for open banking and it has improved the general level of the security of payment transactions through the implementation of strong customer authentication (despite some challenges further highlighted in the following paragraphs and in Section 5.2.8). As noted by a national supervisor, although it is too soon to have conclusive results and robust EU-wide statistics, initial data seem to suggest a reduction in fraud due to the application of the new SCA measures.

According to a national supervisor and a PSP, PSD2 promoted innovation especially in those markets which were under-developed in terms of innovative drive and FinTech solutions: in regions with less developed FinTech hubs, PSD2 unlocked growth in regional innovation hubs and sandbox environments provided through the larger financial service providers and consultant firms. There is less consensus on the innovative drive on those payments markets which were already advanced before the implementation of the Directive (e.g., Nordics and northern Europe). In fact, while the same PSP argued that PSD2 provided a regulatory platform for already established regional FinTech hubs to strengthen and consolidate their market position, the national supervisor noted that the benefits of the PSD2 have been limited in payment markets which were already innovative: for instance, considering security levels, although PSD2 brought some generic benefits from a regulatory point of view, security provisions in the country of jurisdiction of the supervisor were already well developed and PSD2 standards brought no great changes to the security landscape.

All in all, as observed by a PSP, the main benefit of PSD2 is that this piece of legislation (built on the ground of PSD1) provided a foundation and a common set of (albeit imperfect) rules across the EU facilitating the adoption of electronic means in the EU (see more in Sections 5.2.3 and 5.2.4). Non-traditional players that in the past were operating with less clarity are now regulated and provided with clearer roles and obligations. Although the development of innovative models cannot only be attributed to the PSD2, as noted by the same PSP, the Directive created the 'business case' for new business models and encouraged this dynamism.

[174] On the other hand, one national ministry indicated that the emergence of instant payments can create more risks for users as the instant nature of the transaction reduces the time to rectify the payment in suspected cases of fraud difficult. This ministry therefore suggested the need for a regulatory framework over instant payments but highlighted the difficulty of balancing security and consumer protection on the one hand, and ensuring the instant nature of payment on the other.

PSD2 impact on the level of payment services users´ protection

While a more in-depth discussion on the benefits and the limits of this provision is covered in Section 5.2.8 the following paragraphs present a brief overview of the level of security guaranteed by the PSD2 and issues that payment service providers have faced when implementing SCA.

From the evidence gathered from a wide range of stakeholders, it appears that SCA has been successful in establishing a high level of protection for payment service users but stakeholders (particularly ASPSPs and TPPs) have argued that this has come at some cost as a result of regulatory requirements. Some have argued that the legislation and guidance is technically prescriptive, and can be exclusionary as SCA solutions are often restricted to mobile phone users. Additionally, while it has led to more protection, it has also meant more barriers in the customer journey to completing a transaction. Furthermore, loopholes remain that allow for fraudsters to circumvent SCA.

As noted by previous reports, PSD2 introduced changes to the security requirements in order to limit fraud in access to account information, electronic payment initiation and remote channel actions. It further develops the protections initially provided by PSD1 and extends the information obligations to payments to and from third countries in order to ensure the safety of customers' payments funds and other personal data, with the aim in particular of increasing the trust in e-commerce. The obligations regarding consumer protection were specified in the EBA's regulatory technical standards (RTS) on strong customer authentication (SCA) and common and secure communication (CSC). Overall, PSD2 improved consumer protection regarding fraudulent transactions and consumers' rights by reducing liability for unauthorised payments. However, some issues persist, particularly, regarding the application of SCA and its exemptions.

Before the introduction of SCA in PSD2, some Member States, such as Belgium, the Netherlands and Sweden were already using SCAs for electronic remote payments. An EBA opinion from June 2019 noted the difficulties of implementing SCA requirements for market participants that are not payment service providers and therefore allowed NCAs to provide an extension when it came to implementing SCA solutions for e-commerce card-based payment transactions (EBA, 2019). Enforcement on these provisions was therefore pushed back to the beginning of 2021. However, in many markets, such as Italy and Germany, deadlines had been extended further by national authorities to April 2021 (Maus & Mannberg, 2019).

Considering the contribution to levels of protection of PSUs, the literature finds that overall **SCA enhances consumer protection regarding fraudulent transactions**. The notable increase in the quantity and sophistication of cyberattacks in the recent decade made the previously employed single-factor authentication (SFA) and customers more vulnerable. For customers, the increased level of security through SCA means lower risk of fraud and cyberattacks, it can also lead to an increased level of e-commerce activities, especially for customers who were hesitant to make online transactions due to security risks. For card payments, the figures reported by EBA (2021b) for the second quarter of 2020 show that the share of fraud in the total volume of payments is higher for payments that are not authenticated with SCA compared to payments authenticated with SCA. Similarly, for remote payments, the share of fraud in total volume is five times higher for payments authenticated without SCA compared to the payments authenticated with SCA.

PSD2 increases customers' rights in various areas such as reduced liability for unauthorised payments and unconditional refund rights for direct debits in euro. Furthermore, the Directive increases consumer rights when sending transfers and money remittances outside the EU or paying in non-EU currencies. As pointed out earlier, PSD1 only addressed transfers inside the EU and is limited to the currencies of the Member States. PSD2 extends the application of PSD1 rules on transparency to "one-leg transactions", hence covering payment transactions to persons outside the EU as regards the 'EU part' of the

transaction. Inclusion of one-leg transactions aims to provide better information and lower the cost of money remittances as a result of higher transparency. However, literature points out that costumers are generally unaware of the payment procedure and potential risks to which they may be exposed. It is also highlighted that customers are not as sensitive and do not value data elements to the same extent as banks and their regulators due to their lack of education (Brodsky & Oakes, 2017; Deloitte, 2017b).

Overall, stakeholders seem to agree that SCA has enhanced the security of payment transactions leading to a decline in the levels of fraud. The current context is seen as an improvement upon the previous regulatory environment where no authentication was required for transactions. This has been confirmed by survey responses which, as indicated in Annex 2, on a scale from 1 to 5, 21 out of 62 stakeholders indicated that PSD2 contributed to ensuring a high level of PSU protection (rating of 4), and 15 submitted a strong view that PSD2 fully contributed in PSU protection (rating of 5). In fact, only six seemed to believe that PSD2 has to a small extent or not at all contributed in PSU protection.

On the other hand, several merchants and PSPs have noted that the SCA requirement has made the customer journey in a transaction more difficult which can often mean customers do not complete e-commerce transactions. Furthermore, there are a few overarching issues that were raised about its effectiveness, namely, the prescriptiveness of the technologies and the processes required to ensure the correct implementation of SCA.

Several stakeholders consulted, including all types of market participants and national authorities have noted that there remain loopholes in SCA which allow fraudsters to circumvent security provisions. This was elaborated on by a banking association, which noted that the PSD2 requirement of a multi-factor authentication on one hand is very protective of consumers, by imposing 'layers' of security to be passed before a transaction can be finalised (or online account information can be accessed). On the other hand, according to several interviewed stakeholders, there is evidence that fraudsters have found a way to slip into these multiple layers: with SCA relying on different APIs and interfaces, customers can be somehow deceived by false messages asking for personal information or phished via SMS (often used in reality by PSPs to validate transactions). It should be noted, however, that the Commission has indicated that the use of SMS for SCA will be phased out.

Issues have also been raised about the model of SCA chosen. One ASPSP indicated that they had opted for an embedded SCA model (instead of one involving redirection to another interface to perform SCA). While this has put them in line with the preferences of the EBA, it was noted that the embedded model can involve greater phishing risks (for example, because third parties are not required to send additional information that can avoid problems related to phishing). On the other hand, one national supervisor noted that many TPPs have reported low conversion rates rates (number of successful payment transactions and successful instances of payment account access) when the redirection model is applied for SCA even if the redirection websites are fully in compliance with PSD2.

Considering these issues, one PSP argued that PSD2 could instead focus on setting principles and outcomes related to SCA instead of being prescriptive on the RTS and its technology (e.g., biometrics) and processes (e.g., two-factor authentication): in fact, fraudsters' level of sophistication evolves much faster than the timeframe of a regulatory framework which is set to be in place for several years. Another PSP suggested that SCA requirements should follow a risk-based approach with the provider making a decision on the appropriateness of applying SCA for a particular case. This would entail banks and TPPs making their own judgement of whether there should be a risk mitigation measure applied (such as SCA) to a set of transactions based on their own assessment of risk. Under such a model, each party could reject not using SCA. It was noted that this would also remove the need for exclusions. These issues, nevertheless, were not elaborated on by many stakeholders consulted.

Additionally, several national ministries warned of another risk connected to SCA, namely the potential exclusion of certain categories of users from accessing safe and high-quality payment services. It has been highlighted by several stakeholders including consumer organisations that that SCA is often not user friendly, can create friction in the payment process, and has led to a decline in the authorisation of payments. It has also been highlighted by one consumer association that users find they sometimes have to use multiple devices to enact transactions which can be hard for disabled and less digitaly savy users. Furthermore, systems in which six to eight digit codes are sent to the user can be difficult to manage for disabled people using assitive technology. Another issue is that while apps can effectively implement SCA solutions, this has the potential to exclude groups of users who are not digitally savy. In particular, one national ministry indicated that some of the most effective solutions, like biometric authentication factors, are effectively implemented only on modern mobile devices: this could result in an uneven access to quality services for end customers and creates risks of digital exclusion. One national ministry indicated that card readers and "access cards" provided by banks (which request a payer to input a specific set of numbers into the card reader to verify that they are the ones performing the transaction) could help with mitigating this case of digital exclusion and is being applied by some PSPs and ASPSPs. Another example raised by an EU association could involve a solution ASPSPs provide corporate clients. It was noted that when a company opens an account with a PSP, it is provided with a device which is designed to read and recognise fingerprints. The device needs to be linked to the user's computer (through a USB port) and is utilised to implement the inherence factor (which, coupled with the knowledge factor, makes up this particular PSP's offered SCA solution).

PSD2 impact on cross-border payments within the EU

Based on literature review and stakeholder consultation, **this study finds that PSD2 has contributed to a certain extent to developing cross-border payments within the EU and enhancing the quality of such payments**. Nevertheless, an array of stakeholders note that this market was already well developed as a result of the SEPA regulation. Furthermore, literature indicates that small PSPs still face issues in operating cross border. Limited information is available concerning the impact of extending the scope of SCA to one-leg transactions. Additionally, stakeholder opinion on this matter differed with national ministries noting that extending scope is appropriate to ensure similar levels of protection while EU associations argued the EU should adopt international standards instead of broaden scope.

By introducing a European more detailed passporting procedure, PSD2 has fostered the development of cross-border payments market. The passport procedure allows Payment Institutions authorised in one Member State to carry out activities in any other EEA state without additional authorisation. This can be done either through the establishment of branch offices or by the engagement of agents in other Member States or through the free provision of services on a cross-border basis (i.e. without establishing a permanent presence) (EBA, 2017). Many payment service providers in the EU (45% according to EBA survey in March 2019), are either using the EU passporting arrangement or are planning to use it (EBA, 2019b).

The rise of online market platforms, such as Amazon, Uber and Ebay led to increasing demand for cheap and secure solutions for low-value cross-border transactions (Swift, 2018)**.** The entry of non-bank players into the payment markets allowed the development of new digital payment solutions, such as digital wallets with cross-border application, which can facilitate cross-border payments by allowing consumers to operate in multiple currencies (provided the consumers use technology that enables such possibilities such as near field communication).

With this context established, **stakeholders interviewed have suggested that PSD2 contributed to the development and to the quality of cross-border payments within the EU.** Nonetheless, one banking association and several ministries suggested that the EU

legislative framework for facilitating cross-border payments was already comprehensive before the entry into force of PSD2. In fact, it was noted by a national ministry and one survey response that the introduction of SEPA regulation 260/2012 has been a much more significant driver facilitating cross-border payments. Similarly, the survey responses also provided a mixed picture on this matter. Of the 62 responses, 15 stakeholders argued that PSD2 almost fully contributed to the development of cross-border payments, followed by 11 participants who viewed that PSD2 only to a small extent contributed, while 10 others argued that it had no impact to the development of cross-border payments. Comments from survey participants indicated that overall, the EU passport has succeeded in fostering an innovative payments market. However, there is considerable national divergence in how PSD2 has been implemented and interpreted, and this has allowed for regulatory arbitrage given that firms can then passport their service across Europe after having established themselves in one Member State (for which there might be more or less regulatory requirements to do so). These issues are further discussed in section 5.2.5.

Considering the question on whether there was a need for further improvements regarding the transparency of cross-border international transactions within the EU and with other jurisdictions, experts have noted **that some obstacles still exist in the payment markets**. This creates complexities particularly for small PSPs operating cross border, such as difficulties in opening a bank account in Member States other than the host country, diverging AML/KYC requirements across Member States, varying definitions and scope of payment accounts across Member States (EBA, 2019b; Oliinyk & Echikson, 2018).

Although PSD2 aims to increase information and transparency requirements in the European payment markets, the literature stresses that consumer awareness about the new participants, whether they are supervised or trustworthy remains low (EBA, 2021a). The lack of awareness is particularly high when it comes to cross-border transactions within the EU where consumers are often not aware of the classification of the service provided, the provider, the applicable legal framework and the competent supervisors. This can lead to hidden costs due to the termination of the account, or opaque exchange rates with cross-border transactions (EPC, 2021). **This is can be considered problematic as in 2020, the share of fraudulent transactions was significantly higher for cross-border transactions within the EU than for domestic transactions.** More specifically, cross-border transactions within the EU represent 31% of total fraudulent credit transfers (in which a consumer pays money from one bank account to another). Furthermore, it represented 81% of fraudulent card payments reported by issuers (entity providing card to consumer) and 94% of fraudulent card payments reported by acquirers (entities processing payments to a merchant by a consumer). Although their share is relatively small, the payments with counterparts located outside of the EEA are three times more frequently subject to fraud compared to the payments executed inside the EEA. (ECB, 2021c). This indicates that while there are greater risks for cross-border transactions, consumers are at the same time not aware of the trustworthiness of (or the framework and supervision governing) participants providing services in this area meaning they are more susceptible to such risks.

Fostering improved digital identity frameworks is another aspect needed for the further development of cross-border payments. The standards used for electronic identity (eID) and electronic signature (eSignature) services are fragmented across Member States. The eIDAS Regulation facilitates the acceptance of digital/electronic identification for the public sector and private sector, but for the latter, the eID and eSignature solutions are rarely used[175] (ECB, 2021c). However, eID and eSignature services have the potential to foster faster and efficient identification and authentication processes and to fulfil 'know your customer' requirements

Previous literature lacks detailed discussion on the impact of extending the scope to one-leg transactions. However, one underlined aspect is the confusion regarding the

[175] Currently under discussion at the European Parliament and the Council.

application of SCA in case of one-leg transactions card payments where either the payer's PSP (the issuer) or the payee's PSP (the acquirer) is located outside of the EEA (EBA, 2018).

1. In case the issuer is outside the EEA, PSD2 does not require the issuer to use SCA, but the acquirer can still apply SCA, which in turn can lead to rejection of the payment.
2. In case the acquirer is outside the EEA online, PSD2 enforces SCA for transactions. If the acquirer is not SCA-ready, this also leads to rejection of the payment.

Therefore, the EBA has issued a clarification in 2019 for the national competent authorities of the Member States.

In the interviews carried out for this study, stakeholders varied in their responses. Several national ministries argued that if the payments market is being opened up to third countries via one-leg transactions (e.g., an e-commerce merchant seeking to do transactions within Europe), it is appropriate to have open banking requirements and SCA applied as it would ensure a level playing field, protection for consumers, and mitigation of risks. Furthermore, one national ministry indicated that large merchants appear to be circumventing SCA by arranging transactions to be one-leg out even if the transactions are occurring within the EEA.

On the other hand, several EU associations noted that the scope should not be extended. These stakeholders indicated that there does not seem to be a need to extend the provisions currently applying to one-leg or two-leg transactions to currency conversion charges. Moreover, relevant obligations for EU/EEA currencies are already covered by Regulation 2021/1230 of the European Parliament and of the Council of 14 July 2021 on cross-border payments in the Union (codification) amending Regulation (EC) No 924/2009 as regards certain charges on cross-border payments in the Union and currency conversion charges. Thus, as PSD2 aims to facilitate a competitive market for payment services within the European Union, the approach of Regulation 1230 should not be replicated for non-EU/EEA currencies. Furthermore, another EU association argued that the scope of article 82 should not be extended to cover one-leg out transactions as the focus of PSD2 is restricted to the EU. Instead, the EU should monitor initiatives to standardise practices on a global basis (for example, that may be recommended by the Financial Stability Board) and adopt them if they are consistent with PSD2 objectives. Other standards highlighted by other associations include the standards being set by the EPC, OLO, SWIFT GPI, and SWIFT Go. Similarly, an EU association noted that global standards, such as ISO 20022, should not be mandated as the deployment of standards should be decided by industry. It was argued that PSD2 should instead focus on addressing issues *inter alia* regarding cost, speed of execution and liability.

Aside from the issue on scope, national ministries and stakeholders representing the FinTech market noted that the current degree of transparency is sufficient.

Impact of PSD2 on access to accounts by third-party providers

Concerning the impact of PSD2 on access to accounts by third-party providers, the opinions of ASPSPs on the one hand, and TPPs providing AIS and PIS services contrasted significantly. ASPSPs noted frequently that they have faced significant costs in developing access interfaces to payment accounts while there has been little demand for these services on the part of consumers. ASPSPs therefore have argued that they should be able to charge a fee for access to account information. On this issue, caution was expressed by other stakeholders highlighting the potential for uncompetitive behaviour, driving out TPPs from the market, and the potential high costs on merchants. In contrast to ASPSPs, TPPs have argued that they have faced significant obstacles with accessing accounts via ASPSPs' APIs, an issue also raised by some national supervisors. They have stressed that there are poor quality APIs that have not been reviewed by national authorities, and that there are large differences in the APIs across Member States which limits cross-border activity. TPPs have therefore argued that there is a need for more API standardisation and better regulation over ASPSPs to ensure access. Differences are also found on similar lines concerning the extent to which de-risking

plays a role in this issue. ASPSPs note that TPPs are often denied for AML purposes as TPPs have poor control and compliance frameworks. On the other hand, TPPs argue that banks too often use provisions on de-risking as an alibi to restrict access to accounts to prevent competition. These issues are discussed in more detail in this section below.

The Commission Delegated Regulation (EU) 2021/1722 on common and secure communication (CSC) concern the access and use of payment account information and requires that ASPSPs (traditionally banks) should provide at least one form of access to payment account information:

- either through a dedicated interface (via an API[176])
- or through user-facing interface, which is essentially possible through screen scraping[177].

Therefore, PSD2 does not ban screen scraping. According to Recital 20 of the RTS, PSD2 allows for screen scraping as an alternative to providing an API (as noted in the latter point above) or as a 'fall back mechanism' to ensure continuity of services in case dedicated interface fails to provide the necessary access. However, PSD2 makes it clear that TPPs should ensure that they can be identified by ASPSPs as a TPP, so that ASPSPs can take necessary measures and limit the access of TPPs to the extent that the user has consented. The identification procedure of TPPs relies on eIDAS certificates.

Prior to PSD2, API technology was already being employed by social media and online marketplace platforms to make their functionalities available to third parties. This allowed them to create additional value and a dependence on their systems for the access to users[178] (EPRS, 2021). To facilitate the use of open APIs, the European Commission, together with the EBA, created a working group on APIs under PSD2, which lasted from January 2019 to December 2021 (EBA, 2022). During this time, the working group published seven sets of clarifications regarding the use of APIs under PSD2.

Providing payment services through open APIs can bring various opportunities, but also challenges for consumers, third-party providers and banks. Before the implementation of the PSD2, some of the European banks had already started to open their APIs to third-party providers and it was expected that more European banks would start to adopt open API standards as in response to PSD2 (BCBS, 2018). However, the expected move towards open banking has not fully materialised yet (EC, 2020; Rolfe et al., 2021; Worldpay, 2022). Hence, the literature highlights mostly potential benefits and pitfalls of open banking.

As noted by previous reports, open banking can facilitate greater financial inclusion and wider access to more useful and affordable payment services for consumers (Plaitakis & Staschen, 2020). Open banking enables consumers to share their data securely with other banks and TPPs. The entry of PISPs and AISPs in the market has the potential to increase competition, which may consequently lead to lower prices and increased product diversity, which can ensure access to financial services for the segments, which were previously unbanked. Particularly, entry of account information service providers can reduce the information asymmetry faced by consumers and result in better decisions since AISPs can consolidate diverse payment account information and provide consumers with real time analytics.

Increased financial inclusion may also lead to opening of new customers base for new PSPs, which might have been deemed unprofitable for traditional providers. Previous stakeholders' consultations highlighted improved consumer lending as a potential opportunity resulted from increased adoption of account information services. The use of account

[176] An API functions as an intermediary by allowing data transmission between multiple software products and it is described as "open" when it can be accessed by third-party services (Camerinelli, 2017).
[177] Screen scraping is a method to extract data from websites by scanning information displayed
[178] Social media platforms serve as a gatekeeper over key channels of distributions for products and services provided by third-party providers (EPRS, 2021).

information services and data analytics can enhance decision making around lending risks. Having a greater level of customer understanding and the ability to analyse their true financial position more accurately may allow a better calculation of credit risks. In addition, it may also allow credits to be offered to new groups of customers that would traditionally have struggled to access it (such as the self-employed, new/small businesses)(Deloitte, 2018).

However, access to payment accounts requirement can create a competitive imbalance between banks and PSD2 licensed BigTechs, since BigTechs, can quickly dominate to a significant extent the market by combining payment account data with their non-financial services data (such as data on social media, web browsing or e-commerce activity), which they are not required to share with other market players (Carstens, 2022). For instance, Google maintains a payment institution licence in Ireland; Alipay, Amazon and Facebook have E-money licences for issuing payment institutions, acquiring payment transactions and money remittance. Previous studies show that a large majority of banks see BigTechs as the main threat for their businesses, rather than FinTech startups (Borgogno & Colangelo, 2021; Maus & Mannberg, 2019)

FinTechs in the sense of young innovative companies, on the other hand, need to overcome significant competitive disadvantages in terms of compliance costs, brand recognition, high cost of capital and limited information about potential customers (Zernik, 2020). As pointed out by Polasik et al. (2020), the majority of PSD2 licences were obtained by firms already operating before the implementation of PSD2. These firms already had an established brand recognition and necessary capital, and thus an advantage over new FinTechs. However, the potential gains for the (new) TPPs are still realisable. TPPs acting as both AISP and PISP, allowing customers to initiate payments from their accounts via a third-party interface without any (direct) interaction with their banks, can threaten banks' ownership of the customer interface (Borgogno & Colangelo, 2021; Deloitte, 2017b).

Despite the potential competition, a large majority of the banks see the Directive as a strategic opportunity (Camerinelli, 2017; Deloitte, 2018; Maus & Mannberg, 2019). While banks may ultimately lose some control over the use of their customers' data, they can leverage other banks' data by operating as TPP, and reduce their operational costs by building partnerships with other PSD2 players. The 'trusted agent' status that incumbent banks currently enjoy will remain a competitive advantage for some time, and it can be exploited further by offering additional services, such as account information services (Brodsky & Oakes, 2017). However, as of 2019, only around a third of the banks were prepared to take a third-party provider role (Maus & Mannberg, 2019).

The views of interviewed banking and non-banking institutions on PSD2 rules concerning the access to payment accounts converge on the view that ASPSPs (i.e. banks and all financial institutions offering payment accounts with online access) have faced significant costs in developing compliant access interfaces to payment accounts. While a more detailed discussion on efficiency of the PSD2 is covered in Section 5.3, in this paragraph it is worth noting that these costs might have in particular impacted smaller ASPSPs, which, allegedly as yet, have not seen significant demand for access by third-party providers – even if they might more prominently rely on direct access (EBA reference elsewhere check whether they do piggyback on APIs developed by others). The point of view that there has been very little demand for TPP provided AIS and PIS was shared across most, if not all, ASPSPs consulted. Associations of both FinTech providers and banks argue that if PSD2 rules on access to payment accounts are to be further developed, consideration must be given to the potential impact on smaller financial institutions, and whether the cost borne (sunk costs as well as maintenance costs) will result in the anticipated benefits to consumers and businesses. On the other hand, an alternative for smaller ASPSPs, provided for under PSD2, is to allow direct access which would eliminate such costs. Nevertheless, in this context, the opportunity to introduce thresholds have been proposed (e.g., based on volume of payment accounts, volume of transactions) below which smaller ASPSPs or ASPSPs entering new markets could launch and operate payment services without having to set up and maintain

APIs for TPPs to access payment accounts data. However, this might create an uneven playing field between new or small ASPSPs with already established ASPSPs competing in the market. This would also impact *inter alia* the ability of TPPs to offer their services, as AISP, for instance, would not be able to provide information on all the accounts of consumers and access of consumers to the TPP services. TPPs typically do not 'choose' to service only consumers with bank accounts with certain APSPs as this would limit the ability of consumers to use their services, and for PISs, for instance, it would in turn affect their acceptance by merchants. A few ASPSPs suggested that this could also be coupled with an exemption process for those account holders whose payment services and accounts see no demand from TPPs for access. However, this could be complex to set up, and trigger an extended period of time under which TPPs would not be able to provide their services for these ASPSPs (or have to rely on the fallback regime).

Furthermore, while the overall consensus across the different categories of stakeholders is that access to TPPs has been widely granted, several banking associations and ASPSPs noted that the obligation for ASPSPs to provide access to payment accounts data for free might need to be reconsidered. As indicated above, several ASPSPs have argued that the costs of implementing these requirements appear to greatly outweigh the value of doing so for the whole market when APIs had been developed as there has been comparatively little demand in their view for AIS and PIS (with one arguing that AIS and PIS have not emerged in Member States where they were absent before PSD2). Banking associations, echoed by some FinTech providers, argued that the PSD2 review should seek to set a more balanced framework, with a fair distribution of value and risk and the possibility to monetise services by all market participants. They suggested that the possibility to monetise data/services could serve as an incentive for those players that are currently reluctant to provide high-quality, reliable and innovative APIs. Furthermore, they argued that this approach would also be consistent with the recent European Commission Data Act proposal, which featured a principle according to which data holders that are legally obliged to make data available are entitled to reasonable compensation. One ASPSP indicated that it would have been better to have a regulatory framework which allowed ASPSPs to develop APIs for account information access following a request by a TPP to do so and the signing of a contract between the two parties. This would have ensured the APIs were developed with a guaranteed market demand and the possibility of monetising access to data on the part of ASPSPs.

As a way to allow the monetisation of information provision, several ASPSPs and an EU association representing ASPSPs have suggested that Single Euro Payments Area (SEPA) Payment Account Access (SPAA) scheme should be widely adopted in the EU. This would ensure PSD2 remains a baseline for the information that can be provided to TPPs through access via an API, but it would also allow for options beyond the baseline (that can be considered as value-added services) which can be charged for. It has been pointed out by several PSPs that in Finland, ASPSPs have begun charging for access to a high-added value (premium) service in addition to the free-to-access basic API. In either case, a few of the stakeholders in favour of this view argued that such solutions should be developed and adopted by market participants and not be legislated.

On the other hand, considering the issue of whether ASPSPs should be provided the opportunity to charge TPPs for access to accounts, experts have stressed that such considerations should be approached with caution as ASPSPs have incentives to not grant access as PIS compete with credit card services. Such measures could also create undue costs for merchants. In this perspective, it is argued that the level of fees required to counteract incentives to not grant access would be similar to the level of interchange fees, which would make the services of TPPs providing AIS and PIS as expensive to merchants as Merchant Service Charges (MSCs) for processing credit card transactions. Considering the competition related incentives, it was also suggested that ASPSPs could have the opportunity to raise fees for access to accounts to levels that would prevent TPPs from being able to offer

AIS and PIS, suggesting that if such fees are permitted, a discussion should be had on whether such fees should be set by a regulator to prevent market foreclosure.

From the perspective of TPPs, other issues have been raised in terms of access. Most notably, despite evidence that most, if not all, ASPSPs have set up APIs, frictions have been reported by TPPs and national supervisors, due to cumbersome or somewhat complex procedures in accessing payment accounts data. More details on these frictions are discussed in Section 5.2.10. One PSP argued that ASPSPs do not comply with PSD2 and RTS, as they hide some information available in online channels – for example, the name of the customer (available through screen scraping in contrast to current APIs which according to some TPPs only allow access to payment account information, which is also sometimes limited). In another case, a PSP noted that facing obstacles in bank's APIs, they have had to rely on reverse engineering companies to obtain access to bank account information and provide their AIS and PIS. Reverse engineering involves a TPP accessing a payment account by developing an API based on information shared between the PSU and the account holder on the latter's customer interface. It has been noted that this technology involves TPPs storing PSUs' credentials which can entail security and fraud risks.[179] It has also been noted by the EBA that such technology is non-compliant with the RTS on SCA.[180] Nevertheless, this PSP explained that using reverse engineering sometimes means that customers have to perform SCA multiple times (often three times) which degrades the customer journey and has led to some customers not concluding the payments. An additional issue highlighted by a TPP is that many ASPSPs have required them to go through additional registration processes at each ASPSP in order to access their API. This has led to temporary restricted access for TPPs by the ASPSPs. The additional registrations often mean that the TPP must create an account at the ASPSP's API developer portal and submit certain data, such as contact details instead of being granted automatic access. It was noted that access of TPPs to API documentation has been often delayed as ASPSPs validate data from the TPP. This TPP stressed that the EBA has indicated that ASPSPs requiring TPPs to go through additional registration is an unwarranted obstacle, especially if the registration goes beyond what is technically necessary to ensure secure access (EBA/OP/2020/10 paragraphs 47 – 51). It has been argued that any registration steps that go beyond identifying the TPP via the eIDAS certificates could be an obstacle that restricts TPP's access to accounts maintained by the ASPSP and goes against the purposes of the eIDAS certificates, which were to automate the identification process of the TPP.

As a consequence of these aforementioned issues, TPPs have often argued that more standardisation of APIs would be beneficial. Considering this issue, a few ASPSPs have indicated that the current legislation lacks clarity in terms of the standards under which they should develop their APIs. As noted in the survey analysis in Annex 2, stakeholders were asked if only one global API standard would be fit to facilitate payments, and 36 out 62 had expressed a strong view that this should be the case. In fact, only nine seemed to be against this statement, while the remaining 17 responses did not provide an opinion. Stakeholders commenting their opposition to such a proposal in the survey argued that API standardisation could facilitate adoption but may also hamper innovation as banks would be restricted in their ability to develop their own interfaces.

In addition to these obstacles a few TPPs have also argued that PSUs are in some cases actively being discouraged from using third-party providers by their ASPSPs. One case was highlighted in which a PSU informed the TPP that an account manager at an ASPSP contacted the user who had used an AIS and discouraged them from using third-party providers on the basis of data protection.

Evidence that the APIs are not of a sufficiently high quality can be found in the fact that, as pointed out by one PSP, there is a significant portion of the ASPSPs that have not

[179] Yolt. (2022). Understanding APIs, reverse engineering, and screen scraping. Online: Understanding APIs reverse engineering and screen scraping

[180] EBA (2021). Single Rulebook Q&A: Question ID 2021_6044. Topic: Strong customer authentication and common and secure communication (incl. access)

received a fallback exemption (meaning their APIs have not been verified by national regulators for quality, availability and performance). Even among ASPSPs where fallback interfaces are offered, there is still large variability in such fallbacks (which is deemed to be an issue of different interpretations of the requirements). It was argued that clarification on the scope of the fallback exemption is greatly needed, including that it should be made clear that TPPs should be able to rely on any interface offered by the ASPSPs to access the information on their PSUs. Considering the technology specified as a fallback, the PSP highlighted that PSD2 identifies screen-scraping as the fallback technology to be applied when the regulated APIs fail or are unavailable. It was noted that fallback access via screen scraping is just one of the technologies on the market that can be used for account access when APIs are not available or functioning. Therefore, they believe that the Commission should adopt a technically neutral approach to alternative access methods (when APIs are not available) that is not limited to screen scraping. This would allow for interoperability with any external access point or interface (though this would require ASPSPs to publish details on those access points). In this case, it was argued that an ASPSP must publish specifications for all external facing access points or interfaces related to payment accounts to enable TSPs and TPPs to develop interoperability.

Another issue highlighted by TPPs is the quality of sandboxes which have been characterised as differing greatly across banks. One TPP noted that when they have asked for test accounts, around 60% of the banks refused. According to this account, ASPSPs either rejected the request, demanded a fee or referred to the sandbox (which had previously been determined by the TPP to not be of good quality). The TPP noted therefore that there is a need to have a possibility to test operational accounts. In the current circumstances, the TPPs sometimes faces the obligation to launch their products in the market without having tested the accounts.

Issues with APIs have also been raised considering access across Member States. One PSP active both as an ASPSP and as a TPP noted that methods for access to accounts remain fragmented across the EU and therefore continue to be a significant challenge for PISP/AISP to adapt processes to each ASPSP. It noted that a TPP can identify themselves when accessing the interface through an eIDAS certificate. This is based on EU-standards and rules defined in the EU eIDAS Regulation. However, only the German ASPSPs accept the eIDAS certificate without any additional identification steps – all other EU Member States treat the eIDAS certificate like any other private identification certificate and request additional data and information from the TPP.

Issues have also been highlighted concerning PISPs access to account information. Before PSD2, PISPs would be able to access all account information of the PSU and that they were not limited to the data about the initiation or execution of the payment as it argues they are now. Additionally, the directive hasn't in their view been sufficiently clear and thus can be interpreted in a way by the banks that extensively limits the data that PISPs can access. It was highlighted by one PISP, that such institutions need account information data (for example on account holder name and the IBAN number) to determine the risk of initiating the individual payment for the PSU. They also need to know whether the PSU's selected payment account has sufficient funds for the payment initiation. This PISP therefore noted that they would prefer to retrieve this data before the payment initiation has been completed in order to ensure they are not initiating a payment that might be fraudulent. However, they argue that the directive currently doesn't allow for such information to be gathered. Other experts have noted that EU legislation does not provide such a barrier suggesting a potential issue of transposition or implementation at the national level. The PISP added that article 66 of the PSD2 states that an ASPSP shall provide the data immediately after the payment order, i.e. after the payment initiation. Furthermore, they reported that since they are not able to retrieve the information on the availability of funds before payment initiation from the ASPSPs' PIS APIs, they have to rely on their AIS licence in order to retrieve this information for risk mitigation purposes. This is

seen as a shortcoming of the PSD2 directive as PISPs should only have to rely on their PIS licence in order to offer PIS to their customers.

Another important part of information for PISPs is the payment status directly after the PSU has initiated a payment. ASPSPs' documentation concerning APIs have led to uncertainties concerning how to interpret the status of payments. The information on payment status provided by ASPSPs is not clear and ASPSPs have not provided details to clarify the interpretation of data concerning different statuses. This means that it is very difficult for PISPs to know how to interpret them and determine whether a payment will be executed in the end. Furthermore, PISPs have indicated that ASPSPs often do not update the TPP on the status of the payment. On this issue, it was highlighted that the merchant often requests information on whether the payment has been successful, beyond the fact that it has been initiated. Another issue for PISPs is that some ASPSPs allow the PSU to trigger a payment cancellation in the online banking portal for payments initiated in the PSD2 APIs. This in their view is despite the fact that Article 80(2) PSD2 indicates that where the payment transaction is initiated by a PISP, the payer shall not revoke the payment order after giving consent to the payment initiation service provider to initiate the payment transaction. PISPs may not have agreed to the payment cancellation. Furthermore, since the PSU cancels the payment directly via their ASPSP, PISPs are not informed of the payment cancellation. Thus, the PISP will act as if the payment will be executed and they will not become aware that the cancellation has occurred until a merchant notices that they have not received the payment for the product or service that the PSU has purchased. This brings additional risk to PISPs' business models, as they cannot ensure to a payee (merchant) that a payment has in fact been initiated.

It has also been argued by PISPs that there have been cases of increased payment rejections by ASPSPs while utilising the PSD2 APIs. An ASPSP can reject payments, for example, because of the PSU having insufficient funds on their payment account or the ASPSP may have reason to suspect fraudulent activity. Nonetheless, in one case reported by a PISP, they saw a payment rejection rate increase from 1% when using direct access to 40% when they started utilising a particular ASPSP's PSD2 API. They express the concern that while an ASPSP can reject payments that appear to be fraudulent, it could also be that an ASPSP's system discriminates payments initiated via the PSD2 API compared to payments initiated directly with the ASPSP, for example, by ASPSPs applying harsher 'checks' on their own payments. In this context it was highlighted that Article 66(4) PSD2 obliges ASPSPS to treat payment orders transmitted through the services of a PISP without any discrimination other than for objective reasons to mitigate risks.

Furthermore, one PISP argued that customers have encountered IBAN discrimination when wishing to initiate a payment via their payment services. In their account, this happens because the ASPSPs that maintain the PSU's payment account do not allow the PSU to initiate a payment to a recipient's payment account in another country. As a PISP, they need to send to the ASPSP the information required for the payment initiation via the PSD2 API but some ASPSPs may decide to reject the payment initiation instead of executing it as the recipient's payment account is maintained by an ASPSP from a different EU/EEA Member State. It has been noted that this has prevented French PSUs from purchasing goods or services from merchants based in Germany.

Considering these issues, PISPs and AISPs have argued that ASPSPs do not appear to have incentives to remove these problems. ASPSPs are expected to remove identified obstacles within the shortest possible time, and it is the NCA's obligation to take action to ensure compliance with PSD2 and its RTS (EBA/OP/2020/10 paragraph 9). However, it has been suggested that since there are no penalties or sanctions placed on the ASPSP for breaching obligations in PSD2 and the RTS, ASPSPs do not face incentives to comply with the regulations in time which allows them to be non-compliant.

Banks and PSPs seem to have opposite views concerning how ASPSPs and TPPs interact with de-risking requirements under PSD2 and the Anti-Money Laundering (AML) Regulation.

Interviewed banks argued that TPPs often do not meet security requirements which often leads to their access being terminated. One the one hand, under PSD2 banks must provide TPPs access to accounts to be compliant with PSD2 while at the same time, they are responsible for declining clients that are too high risk according to the requirements of the AML: the opinion of some banks is that some TPPs have poor control and compliance frameworks, thus inducing banks to terminate their access to payment accounts. One association of ASPSPs indicated are often unable to get key information from TPPs on safety. This association also argued that information requests from third parties often go far beyond what is required by law.

Some interviewed PSPs argued the exact opposite, highlighting what they perceive as far-reaching use by banks of provisions on de-risking as an alibi to restrict access to potential competitors. According to a PSP, the current PSD2 text does not sufficiently protect TPPs' access. Although there are measures in place that are meant to make sure that access is proportionate and non-discriminatory, in practice this not the case. Such PSP provided an example of how the protection granted to third parties (Article 36) could be strengthened, quoting the case of Denmark: here, the regulatory framework gives guidance to try to make Article 36 of the PSD2 stricter, or to force credit institutions to give more rationale for de-risking, or to notify the regulator when they are off-boarding PSPs or not granting access in the first place. Similarly, one national supervisor indicated similar issues with TPPs reporting that banks too have been too easily restricting access to account information on the basis of GDPR concerns.

Considering the extent to which de-risking has played a role in cases where access was not granted or terminated, based on the experience of some cases of de-risking in some Member States, PSPs noted that although it is difficult to require banks a thoroughly assessed risk-based approach, some stricter measures should be foreseen. The view of these market players is that so far banks are able to use 'blanket' reasons, hinting at some vaguely defined inherent risks, with the objective of thwarting or constraining innovation or entrance into the market.

One PSP involved in remittances noted that non-bank payment service providers such as them have experienced the unilateral closure of their bank accounts across various jurisdictions (e.g., Belgium, Denmark and Finland). The refusal by banks to offer banking services to payment service providers is, in their view, in breach of PSD2 and not consistent with the risk-based approach to money laundering and terrorist financing required by the Anti-Money Laundering Directives. This was considered to be a significant issue as the continuation of this practice threatens to undermine the anti-money laundering and countering the financing of terrorism protections in place by driving payment service providers out of the market and leading customers to use unlicensed illegal channels. In their view, Member States and financial supervisors have not done enough to address the risk posed by these de-risking practices. For example, in many Member States there is no clear process or procedures in place for payment service providers to progress a claim for breach of PSD2 (2015/2366). On this issue, the PSP indicated that they support EBA's January 2022 opinion on the scale and impact of de-risking in the EU which proposed giving itself a mandate to develop regulatory technical standards to clarify the interactions between AML/CFT requirements and the application of Article 36 of PSD2 to ensure more convergence in the way payment institutions access credit institutions' payment accounts services and limited unwarranted de-risking by credit institutions. Additionally, as Article 36 limits the notification process to the onboarding stage, it was argued that the European Commission may wish to consider expanding this requirement to also include decisions made by credit institutions to offboard payment institutions in existing business relationships.

Market challenges and issues related to the implementation and the enforcement of PSD2

As detailed below, stakeholders pointed to a number of issues related to implementation and enforcement of the PSD2. It was highlighted, for example, that the continuous use of Q&As meant new interpretations arising for market actors to adapt to, which meant most stakeholders believed PSD2 left too much room for interpretation. Furthermore, transitional periods for AIS and PIS providers to adapt to new access interfaces was considered to be too short. One issue was also highlighted specific to sectors where payments are not made at the time a good or service is requested. In this case, because PSD2 did not appear to cover such payments, entities from this sector had difficulties finding banks that would take them as customers. TPPs also reported issues regarding long licensing procedures. These issues are elaborated upon below.

Previous studies discuss to a greater extent the problems encountered in the implementation of PSD2 by the PSPs and other market actors, and not as much the implementation and enforcement by national authorities. States failed to meet the transposition deadline for PSD2 arguing that this occurred because implementation had been close to the deadline to implement GDPR. Furthermore, it was argued that this was because in some cases, PSD2 contradicted existing domestic law.

Considering implementation of PSD2 on the part of PSPs and market actors, the majority of online merchants were not ready to become SCA compliant at the time of the launch of PSD2 (though the extent to which this was the case varied across Member States). **The survey conducted by Maus & Mannberg, (2019) shows that the biggest obstacle faced during the implementation of PSD2 for banks was regulatory uncertainty.** Due to the extended deadline for compliance, banks felt that a prolonged period of uncertainty about the rules hindered their implementation process. Other obstacles mentioned in order of importance were:

1. Banks expressed a lack of standards regarding open APIs
2. Limited resources/budget
3. Lack of readiness of TPPs to test interfaces
4. Other (mostly IT related) issues (Maus & Mannberg (2019).

In addition, TPPs reported issues regarding the long licensing procedures and cross-border payment initiations due to technical challenges (Maus & Mannberg, 2019). For TPPs the licensing process is both experienced as cumbersome and was in some cases combined with the underestimation of the requirements to obtain the licence. The long process also implied a delayed testing phase. PSD2 does enable pan European reach for TPPs offering PIS subject to passporting rights. However, in the absence of a single, mandated technical standard for payment initiation, a PISP is presented with the challenge of implementing multiple standards for access to different accounts to initiate a payment. This challenge would therefore limit the network effects of payment initiation services and the development of cross-border payments (Farrow, 2020).

Considering feedback from interviewees, despite the overall benefits brought by PSD2 mentioned in this section, all the categories of stakeholders flagged some key challenges faced in the implementation of PSD2. The most frequently mentioned issues are:

- Regulatory and supervisory fragmentation at national level (Section 5.2.6);
- Lack of clarity on some definitions and interpretations of PSD2 (Sections 5.2.3 and 5.2.4); and
- High costs faced on some key aspects of the Directive, such as SCA (Section 5.3) and provision of access to payment accounts to TPPs (Sections 5.2.3 and 5.2.10).

The vast majority of interviewed stakeholders agreed that the implementation of the Directive was a cumbersome and lengthy process. In fact, the effectiveness of PSD2, according to the wide sample of interviewees, has been stifled by frequent delays in the

deadlines to implement certain provisions (notably on SCA), and by the continuous use of Q&As (e.g., by the EBA). In the latter case, they were seen as useful in facilitating understanding of the legislation and gave supervisors a tool to arbitrate different interests, but continuous Q&As required new interpretations on a rolling basis suggesting such stakeholders did not consider new answers to be consistent with previous ones. In addition to issues in implementation, new interpretations also meant continuous investments to comply with the legislation. It was noted, for example, that business models will need to change to comply with the shift from 90 days to 180 days for the frequency of renewal of SCA. Costs were also involved in having to print and distribute new contracts, communicate with clients on new SCA methods, train employees and obtain legal advice.

This led most stakeholders to conclude that the legal text of the Directive left too much room for interpretation at national level and by each category of stakeholder. Despite the inherent characteristics of a Directive, which is subject to transposition at national level by its nature, there is a wide consensus across the table on the need for clearer guidelines, especially on the key concepts mentioned in this section.

The key risk highlighted by most stakeholders is that, due to this level of uncertainty, **the market uptake and the innovative potential of PSD2 have not been fully exploited so far.** This is particularly evident in the different interpretations of registration requirements by national supervisors, leading to significant discrepancies in the complexity of the procedures across Member States (as discussed in Section 5.2.6).

Similarly, it was highlighted by one supervisory authority that entities that were already acting as PIS and AIS providers under PSD1 in their Member State faced huge challenges with the technical migration to the new access interfaces required in a short timeframe. The transitional periods foreseen in PSD2 underestimated the necessary time for testing and the actual migration. This resulted in the need for more resources than expected.

Another issue highlighted by a merchant association applied specifically to sectors where payments are not made at the time the good or service is requested (e.g., travel cards, fuel cards, and segments of the hospitality sector, in particular, hotels). To take the example of hotels, payments are not always made at the time of the booking. Instead, an imprint of the credit card is taken to ensure its validity and to block any guarantee for future payment. They have therefore found that banks sometimes refuse to take up hotels as clients because their usual form of payment is, according to the association, not covered by PSD2. Hotels have therefore found that they need to rely on third-party PSPs to be able to receive payments but these involve higher costs than traditional banks which the association indicated would lead to higher prices imposed on the consumer. This is seen to also reduce competition, as the number of PSPs and banks that have knowledge on the specificities of the hotel sector and that are willing to provide services to the industry despite not being covered by PSD2 decline becomes more restricted. On a broader note, one national supervisor indicated that clarifications are needed about the requirements applying to beneficiary-initiated transactions (MITs) such as the case of hotels. It was noted that more clarity was needed over the role of consumer mandates for payment (considering whether it is paper-based, remote-digital, or others) for the application of SCA.

An issue was also raised about whether the Directive applied to the services provided under the LNE. One PSP indicated that the EMI and PI regulatory regime requires them to meet robust outsourcing and operational resilience requirements which appear to be tailored towards the supervision of retail banks and are not applicable to their business models (such as the provision of travel cards and fleet cards). They are therefore seen as unnecessary administrative burden for their businesses.

5.2.2. Objectives of PSD2

What were PSD2's main objectives? How far has each of these objectives been reached?

The aims of the PSD2 were to:

- Improve competition and cross-border payments;
- Contribute to a more integrated and efficient European payments market;
- Further level the playing field for payment service providers by including new players;
- Make payments safer and more secure; and
- Enhance protection for European consumers and businesses.

Overall, it appears that there have been important improvements in the payments market in regards to meeting the above described objectives of PSD2 but certain issues have prevented these objectives from being met to their fullest extent. These are summarised below.

As indicated earlier, competition appears to have increased as new market players have entered the market which has provided alternatives to legacy businesses and pushed the latter to innovate alongside the new entrants. Tied to the issue of competition is the issue of a level playing field. It can be argued that this only was partially improved as larger players, especially BigTechs, still have advantages over smaller players and FinTechs still face substantial obstacles. Furthermore, as noted above, PSD2 licensed BigTechs could in theory significantly disrupt the market by combining payment account data and non-financial services data, which creates a competitive imbalance with banks.

It can be argued that the integration of the European payments market has improved as cross-border payments have also increased with several stakeholders indicating that PSD2 has allowed them the possibility to passport their licence and provide services across borders. Nonetheless, as highlighted below, there are issues across the Member States as different national authorities demand different regulatory requirements of PSPs operating across borders which has made such activities difficult. Considering the efficiency of the market, there are still issues present as TPPs face difficulties accessing ASPSPs APIs, which are often considered to be inadequate, and ASPSPs in turn have in their view faced significant costs involved with developing such interfaces.

Considering the aims 4 and 5, the findings presented above appear to indicate that the level of protection throughout the market has increased. This is demonstrated by the decrease of fraud rates reported by several PSPs and EU associations (findings in Chapter 3 on market developments indicate that fraud rates in western EU countries remained stable but fell in other Member States). Nevertheless, some stakeholders indicated that loopholes in SCA remain. On the other hand, the effectiveness with which the overall decline in fraud rates has occurred has been questioned by several stakeholders as PSPs have found difficulties with meeting regulatory requirements and these have in some cases, according to interviewees, meant a slightly negative results in the market. Concerning the former, as noted above, PSPs have found difficulties with the correct implementation of SCA. Considering the latter, as noted above, SCA has meant increased instances of transactions not being finalised by the user due to a lack of a smooth customer journey.

Level of compliance of businesses

Overall, while there were few interview responses to the question concerning the extent of compliance, some ASPSPs and ministries suggest that compliance is high – although this might not be representative considering issues discussed above, particularly concerning smooth access of TPPs to accounts through APIs. TPPs argue that ASPSPs are not compliant as they are in effect not allowing access to accounts for information or payment initiation by having poor quality ASPSPs and that these issues are not being addressed by them.

Furthermore, national ministries interviewed indicated that there was overall a high level of compliance on the part of all actors involved in the market. Some national ministries highlighted difficulties with fulfilling SCA obligations but that ultimately there is compliance with the requirements. As discussed in later chapters, it was highlighted by national ministries that high levels of compliance are also found with regards to allowing access to third-party providers but the quality of access is questioned by TPPs. Nonetheless, one PSP did report that in Luxembourg some banks had informed them in March 2022 that APIs were not ready to be used suggesting anecdotal evidence of a lack of (or delays in) compliance.

It has been suggested by a German consumer association that there may be a low level of compliance when it comes to liability obligations for PSPs, with PSPs (and banks in particular) circumventing rules established under Article 73 (1). In the case of Germany it has been highlighted that a loophole is potentially established by the §§ 675v BGB ("Civil Code (BGB) Section 675u, Liability of the payment service provider for unauthorised payment transactions") which applies to cases where unauthorised debit transactions have occurred on customers' accounts. According to the law, banks have to refund the payer immediately, or on the following business day at the latest. Exemptions only apply in the case of suspicion of fraud that banks report to the national authority in writing. However, citing § 675v BGB, banks avoid liability in practice by regularly alleging gross negligence on the payers' side (with the PSP adding that this is done without sufficient proof). It was noted that at times the onus is placed on consumers to prove before a court that they have not engaged in gross negligence, which entails large legal fees in addition to loss of funds from the fraud that has previously occurred. It was added that to ensure that article 73 is relevant in protecting consumers, it should be clarified that PSPs have to refund payers irrespective of disputed allegations.

Operational and security risks

As indicated in Annex 2, most survey respondents believed that operational and security risks are addressed (rate of 4/5), with 21 out of 62 responses noting this was the case. Furthermore, of these 62, 12 stakeholders strongly argued that they have been fully addressed (rate of 5) and 17 argued that operational and security risks are to some extent addressed (rate of 3). Nonetheless, some respondents indicated that consumers are increasingly using non-regulated financial models such as cryptocurrencies, exposing the financial system to other significant risks. Furthermore one respondent indicated that front line staff of banks are unaware of the existence and specificities of PSD2 which means that if end users are facing issues related to services delivered as part of PSD2, support line staff are unable to handle requests for assistance.

5.2.3. Scope of PSD2

Widening of scope

PSD2 widens the scope of PSD by covering new services and players. PSD2 introduces two new regulated payment services: payment initiation services (initiating an online payment order), and account information services (online services to provide consolidated information on one or more current accounts).

It also outlines two new types of regulated TPPs that will be granted direct access to customer accounts: Payment Initiation Service Provider (PISP) and Account Information Service Provider (AISP). Banks and similar institutions are denominated as Account Servicing Payments Service Providers (ASPSP) to emphasise the difference between institutions that hold customer accounts and new players that merely access them

The geographic scope has also been widened to include:

- Intra-EEA payments (two-legs) in non-EEA currencies
- Payments to and from EEA (one-leg in or out) in any currency

Narrowing of exclusions

Finally, various existing exclusions under PSD1 have been narrowed or clarified, including the exclusions for ATM operators, commercial agents, use of payment instruments within a limited network and electronic communication network providers.

A range of stakeholders (including policy makers, banks, TPPs) have argued that the scope of the Directive should be extended to cover the full extent of the payments market, taking account of trends such as crypto/ digital currencies, (in their view) growing prominence of FinTechs and BigTechs[181]. Banking sector representatives were particularly in favour of bringing FinTechs and BigTechs within the fold of the Directive. More and more (technical) service providers are engaging in the payment transaction value chain, but are not regulated under PSD2. Card wallets in the form of mobile applications (most often applications supported by Google, Apple or Samsung) provide an interface for initiating card payment transactions at POI. These services are based on the tokenised card. The providers of such wallets are considered technical providers and are not required to obtain licences as payment service providers. The authorisation and the billing process of such instruments remains the same, which means that wallet providers do not open payment accounts and do not enter into possession the funds of transactions. Nevertheless, these technical providers de facto are in control over the channels that consumers use to make payment transactions and therefore are very important for PSPs that wish to connect cards issued by them to such channels (wallets). This matter is significant not only within the wallet applications but also for technical and often innovative payment solutions which could use application or hardware elements for authentication processes, such as fingerprint reader, face recognition etc. PSPs argue that their restrictive practices have limited innovation. Access to richer OS/device controls is essential for PSPs to offer convenient and secure payment services, especially on mobile devices. Device manufacturers' blocking of such access distorts competition as rival PSPs cannot make use of these technologies, which are exclusively used by OS operators to provide their own payment services. Policies around cookie or device identifier storage by some device manufactures, moreover, can also be restrictive for PSPs.

In the same vein, some interviewees noted that some form of regulation and supervision of Technical Service Providers (TSPs) and payment processers (e.g., iDeal[182], for example, does not fall under PSD2) should be part of a general payments framework (while not necessarily bringing these actors within the fold of PSD2). More and more TSPs are engaging in the payment market – on both sides: the 'front-end' (e.g., interfaces between payer and payee) and the 'back-end' (technical services for the PSP itself). These services normally do not offer any transfer of funds and are therefore not directly involved in the transaction. Primarily risks of front-end services could occur with regard to privacy, data-protection, competition, cyber-security. At the back-end technical services could also may affect financial stability

PSD2 does not regulate services provided by technical providers, including data processing and recording (e.g., provider of core banking hosted in the cloud; technical acceptance provider providing payment terminals; providers of SCA solution (authentication control servers and authentication devices); providers of front-end payment solutions such as the X-pays. As an example, the X-pays provide services that are very close to payment initiation services (they effectively control the initiation stage of the transaction and the authentication of the PSU). Bringing them into the regulatory perimeter of PSD2 would create a level playing field with PISPs, but also with ASPSPs with which they have contractual reliationships. PSPs have little control over the security and processes of these front-end solutions, even though they bear the responsibly for the security of the transactions. The EBA clarified that issuers can rely on the authentication solutions integrated in smartphones, such as fingerprint readers, provided

[181] Although some BigTechs – such as Google – have licences for offering payment services under PSD2 in the EU, they often act as technical service providers (which do not require a licence), and they work together with current licence holders such as banks or payment card schemes in order to offer their payment service (e.g. Apple).
[182] an e-commerce payment system used in the Netherlands, based on online banking

that the PSPs ensure compliance with the applicable legal framework (the smartphone needs to have a satisfactory level of security and mitigating measures to ensure the independence of the authentication elements have been applied and the security measures needs to be documented, periodically tested, evaluated and audited in accordance with the applicable legal framework). This covers specific cases where applications of the PSP installed on the mobile device use the underlying technology, but there is an interaction between the PSP and the mobile device. However, there is not a contractual relationship between the PSP and smartphone manufacturers when the smartphone is used for applying SCA. The control of the SCA may be with the mobile phone manufacturer, which gives rise to potential concerns in case PSPs do not apply any controls or checks on the security measures and their compliance with the requirements of PSD2 and the RTS on SCA&CSC. Hence, bringing digital wallets providers (i.e. mobile phone manufacturers providing payment initiation services and SCA solutions) within the scope of PSD2 may close this regulatory gap and introduce security requirements for these actors.

Moreover, stakeholders highlight that the role of some of these providers, has become essential in the provision and in the security of payment services, especially digital payments. As such they are essential for the proper functioning of retail payments and may be deemed 'systemic'. As their governance authorities have generally no direct relation with the final payment services users (neither merchants nor consumers), there is no rationale for qualifying them as payment services providers. However, due to their systemic importance for the retail payments market, they should be, as is the case for financial market infrastructures like Central Counterparties (CCPs) and Central Securities Depositories (CSDs), subject to an ad-hoc authorisation and supervision regime within the remit of the euro system. It was suggested that proper authorisation would allow greater leverage regarding the compliance of payment systems and schemes with EU regulations (including bringing them under DORA) than with moral suasion, and would also be necessary to enforce their legal establishment within the EU. Nevertheless, this would have to be well articulated with the current ECB/Euro system regulations covering market infrastructures in order to avoid overlaps.

Box: Role of Big Tech in the payment services market in Europe

There are differences in the approach that each BigTech is taking to develop and provide payment services in Europe. For example, Apple is developing new payment capabilities through partnerships with incumbents of the financial sector (i.e. Apple Wallet), whereas Facebook is developing its own digital currency. BigTechs also differ from each other in the roles they take in the payments ecosystem. Some function as intermediaries between clients and suppliers to facilitate payments on their platform, while others issue electronic money directly to clients.

Most BigTechs chose an Electronic Money (E-Money) licence in the European market. Apple Pay does not have a payment licence in Europe. Through partnerships with licensed local banks, Apple Pay is able to provide contactless purchases in stores with Apple devices. Likewise, although Tencent (WeChat Pay) holds no payment related licence in Europe, it is able to service Chinese customers through partnerships with companies in the EEA (i.e. the Parisian rail company, RATP).

Table 8: Overview of BigTechs with a payment licence in Europe[183]

BigTech	Year EEA payment-related license acquired	EEA National Competent Authority
Licensed in Europe		
PayPal (Europe) S a.r.l	2007 (Banking License)	CSSF (Luxembourg)
Amazon Payments Europe S.C.A.	2010 (E-Money License)	CSSF (Luxembourg)
eBay S a.r.l	2014 (Payment Institution license)	CSSF (Luxembourg)
Rakuten Europe Bank	2016 (Banking license)	CSSF (Luxembourg)
Facebook Payments Intl Ltd.	2018 (Payment Institution license)	Central Bank of Ireland (Ireland)
Alipay (Europe) Limited S.A.	2018 (E-Money License)	CSSF (Luxembourg)
Airbnb Payments UK Ltd.	2018 (E-Money License)	FCA (United Kingdom)
Google Payments Lithuania UAB Google Payments Ireland	2018 (E-Money License) 2019 (E-Money License)	Lietuvos Banka (Lithuania) Central Bank of Ireland
Uber Payments B.V.	2019 (E-Money License)	De Nederlandsche Bank (Netherlands)
Takeaway.com	2019 (Payment Institution)	De Nederlandsche Bank (Netherlands)
Zalando Payments Solution	2019 (E-money License)	BaFin (Germany)
Licensed outside Europe		
Apple	Apple has payment licenses in the US.	United States of America
Tencent	2014: Banking license in China 2019: E-Money license in Malaysia & 2020: Virtual bank license in Hong Kong	People's Bank of China, Central Bank of Malaysia Hong Kong Securities and Futures Commission
No license		
Microsoft	No payment license	-

Source: Laurens van der Spek MSc and Sebastiaan Phijffer MSc Ing. Will biotech's change the European payments market forever?[184]

There are mixed views on whether it is appropriate for AISPs and PISPs to be kept under the scope of PSD 2 or not. Some interviewees argued that AISPs and PISPs should not be classified as payment institutions, as they they do not hold or handle any funds. This results in them being subject to a broad set of AML requirements even though no handling of customer funds is involved. Then there were those who argued that TPPs who are AISPs only should be excluded from the scope of the Directive suggesting that there should be some separation between payment services and data services. According to these stakeholders, AISPs do not initiate or execute payments; they only access the account information. Thus, the risk of fraud from AIS is minimal if at all. Still, access to account information requires that the user performs an SCA. Any unnecessary use of SCA results in increased inconvenience for the PSU in the form of a sub-optimal user experience without any added risk mitigation. Furthermore, even though AISPs are not involved in movement of funds, they are also subject to AML regulations as a knock-on effect of having been included under PSD2.

Mostly, it was argued that AIS should remain under the scope of PSD. The fact that AIS is handling funds is not crucial in this context, because AIS is often an integral part of the payments' related value chain, and the players behind related services i.e. ASPSP, PIS, PSP. The AIS service relies on access to highly sensitive personal and financial data and therefore

[183] BigTech licences for payment subsidiaries in the EEA derived from the EBA register of payment and electronic money institutions under PSD2
[184] https://www.compact.nl/en/articles/will-bigtechs-change-the-european-payments-market-forever/

there is a reasonable risk that this information can be used by unauthorised entities or for unauthorised purposes (fraud, unwanted marketing etc.). As such access to this data should be limited to regulated entities. Several stakeholders expressed concerns that de-scoping AISPs out of PSD2 at this stage could result in unnecessary implementation challenges. For example, it could potentially lead to ASPSPs blocking account information access and threaten the data parity principle that currently exists within PSD2. With PSD2, PSUs have the right to make use of AISPs services, and hence AISPs have a right to offer their service to PSUs. If there were no regulation in place, then many ASPSPs would not be obliged or incentivised to continue to support AIS services. ASPSPs may even block AISPs from accessing account information. Additionally, due to the fact that PISPs usually cannot fully rely on their PIS licence to provide their services to PSU, due to risk mitigation purposes, PISPs have used AIS licences to retrieve account information to enable this. Should AIS not be covered by PSD2, PISPs would have to live with only being provided with very limited data concerning the account. This would be very damaging to PISPs' services. This topic is discussed further in the following section on the clarity of the PSD2 definitions.

Stakeholders expressed some concerns regarding Limited Network Exclusion. Firstly, it was pointed out that PSD2 led to divergent implementation of this exemption across Member States. Although a new EBA guide on the application of the limited network exclusion has recently been published, it still leaves some room for interpretation and this needs to be addressed. There are, for example, different requirements in terms of timelines, details that service providers are required to provide as part of the activity description, or the frequency of the submission in the various Member States. Notification forms vary from being short and standardised paired with prompt reactions from the responsible competent authority (the example of Italy was provided as characteristic of this approach) to very burdensome ones that require the continuous submission of information over an extended period of time. One EU association contrasted the case of Belgium, for which no legal forms were required to be recognised as part of the limited network exclusions, with France for which the administrative burden was significant. This was also highlighted by a few PSPs which indicated that French authorities required extensive engagement and large amounts of data to be provided, including around security of funds. It was argued that clarity over requirements and cooperation with EBA and other Member States would be potentially beneficial in resolving these discrepancies. One NCA mentioned that according to the new guidelines, services with limited risks for consumers should be excluded, even though the volume of money is high. Secondly, it was pointed out that those benefitting from this exemption are not necessarily small market players. For example, market feedback shows that the number of exempted payment institutions in France, which are not only small market players, rose sharply in recent years to reach 80 by 2021, including notably major food delivery and telephone service providers, and almost 1,700 in the EU[185].

The exemption has led to a situation that some major market players in the field of payment services are currently left out of the picture for competent authorities, which may generate risks for customers (e.g., inadequate consumer protection). The PSD should consider setting a threshold for the volume of payment transactions (to be determined) above which a firm can no longer benefit from the exemption under PSD2 and must therefore be authorised. In this context, strong arguments were made by some stakeholders against bringing fuel cards within the fold of PSD.

There are reportedly divergences and lack of clarity as regards the application of commercial agent exclusion. At European level, there are different definitions of a commercial agent. Some stakeholders mentioned that the perimeter of the exclusion related to the commercial agent, described in Article 3(b) of PSD2, should be better clarified to avoid uncertainty in case of payment transactions carried out by the platform's operator. In this case, it is difficult to understand if the operator of the platform acts on behalf of both the payer and

[185] Mara, B. and Perney, P. (2022) PSD2: EBA publishes its final guidelines on the limited network exclusion. Accessible here

the payee, or If it represents only one of them. Only in the latter case, it is possible to apply the exemption set out in Article 3(b) and the commercial agent can transfer the funds between the parties. In this regard, the PSD should detail the condition to be fulfilled by the agent to operate out of scope.

A review of the limits set under telecommunications exemption may be warranted. Telecommunications providers, especially mobile operators, are seeing a strong increase in demand for the billing of digital goods. This is due to the increasing use of smartphones as well as the fact that more and more innovative digital offerings are being developed (with more high-quality and therefore more expensive content, such as security packages or streaming offers, being offered for use with mobile devices). In this context, the limit of EUR 300 is quickly reached by consumers. It was suggested that an adjustment of the threshold and the limit in Art. 3 lit l PSD 2 is warranted in light of these developments. An increase in limit would promote the further development and growth of the market for digital goods.

Finally, many stakeholders are in favour of merging EMD and PSD2, but there are also arguments against this. Many stakeholders have argued that the distinction between e-money institutions and payment institutions is gettingg blurred with both offerring increasingly similar services that customers are unable to distinguish (payment services vs e-money services). This creates a potential for companies to exploit the differences between PSD 2 and EMD (e.g., capital requrements). Merging the two regulatory regimes (e.g., by including e-money services in annex 1 of PSD2), would reduce the overall complexity of the legal framework, avoid regulatory arbitrage, ensure technological neutrality, level-playing field and a future-proof legal framework. Arguments against merging EMD and PSD 2 are as follows:

(i) E-money is a product while payments are a service. It was pointed out that some MS/competent authorities are confusing e-money with payment accounts. E-money, for example, is money on a debit card, but having money on your payment account is a different concept, i.e. a deposit, and therefore entails different risks.

(ii) E-money can enable more innovative constructs (as e-money are funds distinct from underlying funds). E-money is not a deposit or debt instrument, and consequently attracts its own legal treatment. It can be purchased and sold, and it is pegged against national currencies at par, with a right for redemption also at par. The concept of an e-money institution (EMI) under the EMD2 makes financial services more accessible and efficient for a broad range of commercial and private customers. Being more agile and fast in their operations, EMIs are offer an alternative to traditional banks and provide a wide range of unique benefits to customers. Some stakeholders were worried that by merging the two directives, e-money would lose its flexibility.

Considering that e-money covers a broad range of activities (including pre-paid cards and vouchers, online and mobile wallets, and e-money tokens), which all have different associated risks, a stakeholder called for greater delineation of the different types of e-money activities and for specific, targeted regulatory treatment for each, that could address the pertinent regulatory and market risks applicable to each activity, including from consumer protection and financial crimes perspectives. Such clear categorisation of e-money activities would also allow for a greater level of activity-based disclosures and disclaimers and would accordingly assist with transparency and risk awareness from a consumer perspective.

5.2.4. Clarity of the definitions used in PSD2

This section first provides a literature review on the adequacy of current categories of payment service providers considering developments in the payments market. It then provides stakeholder feedback on whether the definitions included in the PSD2 ensured enough clarity to the different stakeholders impacted by the Directive, and whether such definitions are still fit for purpose. As discussed below, TPPs argued that definitions of AIS are too narrow considering the services that they could offer to consumers based on the latter's consent. Furthermore, it was argued by several types of stakeholders that in the long-term definitions

of AIS should be put into the scope of a new Open Finance framework rather than PSD2. Several different stakeholders also noted that definitions should not treat remote payments and non-remote payments as distinct as in practice the forms of payments overlap. Issues concerning lack of clarity were raised following the CJEU case DenizBank AG v *Verein für Konsumenteninformation* case.[186] On this issue, it was argued that unclarity emerged over the definition of a payment instrument, the application of SCA rules, and the division of liability for unauthorised payments. When it came to the concept of e-money, most stakeholders argued for a merge of EMD and PSD2 as they e-money and payment services are not distinguished by PSUs, though a minority of stakeholders argued to keep them distinct as risks faced by the EMIs and PSPs are different.

Accuracy and relevance of definitions in light of market developments

According to stakeholders interviewed, there is a general consensus that the definitions used in PSD2 are still accurate and relevant, but stakeholders surveyed nonetheless flagged in particular a key issue about the interpretation of definitions. As noted in Annex 2, based upon the market developments, from the 62 stakeholder responses, 26 agreed that the definitions specified in Article 4 of PSD2 are still accurate and relevant. Only 17 rather claimed that the definitions of Article 4 are not accurate, with the remaining 18 having no opinion on the matter.

Clarity and uniformity of application of PSD2 provisions

As highlighted in the analysis of survey responses, there is a division of opinion concerning whether definitions contribute to a clear and uniform application of PSD2 provisions. Some 24 claimed that the definitions do contribute to a clear and uniform application, while 23 expressed that it does not, while the remaining 14 had no opinion.

As observed by several stakholders, the clarity of PSD2 appears to be affected by two main problems: the lack of consistency in the interpretation of some definitions by national competent authorities, and the choice of excluded providers.

Surely the most controversial across all stakeholders is the definition of "payment accounts": this is a key definition to clarify which accounts ASPSPs are required to provide access to and which accounts are subject to SCA requirements. As noted by a PSP, this source of uncertainty prevents a uniform application of PSD2 provisions. For example, France is the most frequently mentioned Member State in which credit cards are classified as payment accounts, whereas in other countries they do not have such classification. The PSP argued that it would be helpful if PSD2 clarified that the requirements around SCA apply to 'payment accounts' through which payers are able at least to place funds, withdraw cash, and execute and receive payment transactions, including credit transfers, to and from a third party, i.e., those used primarily for the execution of day-to-day payment transactions. This also creates issues in terms of third-party access. As noted by several PSPs, in France, as credit cards are classified as payment accounts, TPPs are able to access account information related to these cards. In other Member States such as Spain, credit cards are not considered payment accounts and so are not accessible. This is considered to also have an impact on consumers as it means protection measures under PSD2 (such as SCA) are not required for these accounts. Other Member States that consider credit card accounts as payment accounts include Sweden and Finland, although in Sweden, PIS are not applicable to card payments as initiation is considered to be only applicable for payments initiated by the payer. On the other hand, credit card accounts that allow for the possibility for credit transfers are under the scope for PIS. As noted earlier, in any case, several PSPs noted that many of

[186] Judgment of the Court (First Chamber) of 11 November 2020. DenizBank AG v Verein für Konsumenteninformation. Request for a preliminary ruling from the Oberster Gerichtshof. Reference for a preliminary ruling – Consumer protection – Directive (EU) 2015/2366 – Payment services in the internal market – Article 4(14) – Concept of 'payment instrument' – Personalised multifunctional bank cards – Near-field communication (NFC) functionality – Article 52(6)(a) and Article 54(1) – Information to be provided to users – Change in the conditions of a framework contract – Tacit consent – Article 63(1)(a) and (b) – Rights and obligations related to payment services – Derogation for low-value payment instruments – Conditions under which applicable – Payment instrument that does not allow its blocking – Payment instrument used anonymously – Limitation of the temporal effects of the judgment. Online: Case C-287/19

these accounts that are not considered payment services (e.g., investment savings account, and credit accounts) but are seen this way by the users. As indicated by survey responses, several TPPs therefore argued that the definition of "payment accounts" should include savings accounts, credit card accounts to achieve full potential (although the former does not allow payments to be initiated).

Another PSP argued that the definitions of "payment account" and "acquiring of payment transactions" could be improved in terms of clarity and to narrow its scope as the definitions are currently being interpreted excessively broadly resulting in certain low-risk activity that should be unregulated being deemed to require a payments licence. An example was given concerning the collection of tips (gratuities) by a merchant for its staff. It was noted that it is possible to stretch the definition to have this be deemed to be a regulated service under current definitions and if this were to be regulated it could be subject to a wide array of other requirements such as open banking TPP provisions.

One PSP addressed specifically the issue of whether the definitions are appropriate considering market developments. With the evolution of some of the payment services and the emergence of new and innovative business models, there is some degree of uncertainty in the market in relation to the interpretation of various payment services. It was noted for example, that the term 'electronic payment transaction' has not been properly defined in PSD2, which raises challenges regarding the interpretation and application of various provisions, notably in relation to the regulatory treatment of mail and telephone orders (MOTO transactions). It was added that guidance provided in Recital 95 of PSD2 is insufficient as all payment transactions (except cash) have an electronic component in their execution. To further elaborate on this issue, the PSP highlighted the case of an online booking. This can be considered an electronic payment but if the booking platform sends the hotel card details in paper format, in the opinion of the PSP it is unclear whether this can still be considered an electronic payment.

Other issues mentioned by a national supervisor relate to some business models such as 'buy now and pay later': it was argued that it has not been clear if they should be considered payment services or if they should be considered as consumer credit services (in the Commission's 2021 legislative proposal to revise the Consumer Credit Directive, 'buy now and pay later' services are brought into its scope). In addition, another problem observed by the same national supervisor concerns providers that act under what is called "white label". It is not clear if these providers are agents, distributors, and what position they play in providing payment services.

Payment services, Payment Initiation Services and Account Information Services

There are conflicting views considering the definition of services covered in PSD2. TPPs consider definitions to be too narrow in scope restricting innovation and possible services for consumers. Some ASPSPs believe AIS should not be defined in PSD2 while others note that investments in implementing APIs to allow account access for AIS and PIS represent sunk costs. Definitions concerning types of payments (e.g., debit payments, and credit card payments) are considered clear but may require ammendments considering new market developments.

Another issue for which concerns were raised was about the use of third parties by ASPSPs. One association noted that ASPSPs are contracting third parties to develop and maintain banks' online interfaces that provide their customers information on their accounts held with this bank (such as balance sheet information). It was argued that this does not constitute AIS and that the definition should remain restricted to "the provision of information on accounts held with another PSP or more than one PSP" as it is currently defined in PSD2.

Another issue highlighted concerned the definition of remote and non-remote payments in PSD2 considering new market developments though there was a difference in opinion as to

whether this should entail a greater distinction between the two or removing the distinction. Several national supervisors indicated that for payment options based on new technology, such as smartphones, mobile apps, and wallets, it is difficult to distinguish local payments from remote payments. When a smart smartphone is used for the initiation of a remote payment transaction, it can be initiated via the internet for e-commerce but it can also be initiated at a physical point of sale (including for the authentication of the PSU) but carried out through the internet (e.g., with a smartphone). Payment transactions can therefore be based on local and remote connections at the same time (this can also include through QR code interaction, mobile POS, etc.). One national supervisor therefore argued that the distinction between local and remote payments is no longer relevant and so the distinction should be removed in future legislation. On the other hand, another supervisor interpreted this finding to mean that a clear distinction is needed to differentiate the two forms of payment. As remote payments require SCA to be performed on them, clarification either by removing the distinction between the two concepts, or clearly defining the two concepts in light of new market developments would better specify which transactions should be covered by SCA.

Other definitions highlighted in survey responses that may require clarification include “unique identifier”, which could be reworded to avoid ASPSPs making use of this definition to avoid access to accounts. Article 4 (32) highlights that “sensitive payment data” refers to, “data, including personalised security credentials which can be used to carry out fraud.” It was highlighted by experts that there should be no barriers to access since, in reference to this concept, Article 4(32) indicates that “for the activities of payment initiation service providers and account information service providers, the name of the account owner and the account number do not constitute sensitive payment data”.

Furthermore, the definition of “authentication” was seen as inconsistent as there were different interpretations over whether the term should go beyond identifying a payment service user. According to Article 72(1) of the PSD2, the PSP has the obligation to prove that the payment transaction "was authenticated". This was argued to be conceived as incoherent with the definition of authentication. Article 4(29) of the PSD2 stipulates that authentication is conducted to identify the user, not the transaction, thus there is no "authentication of a transaction". Other experts disagreed noting that this understanding of the legislation is incomplete as Article 4(29) adds that authentication “means a procedure which allows the payment service provider to verify the identity of a payment service user” but also “the validity of the use of a specific payment instrument, including the use of the user’s personalised security credentials”.[187]

On the issue of potential overlaps, most stakeholders consulted noted that there are no overlaps or gaps concerning the service categories of payment initiation service, account information service and the acquiring of payment transactions. The main issues concerning these categories were more to do with clarity and interpretation of the definitions on their own rather than overlaps or gaps in the definitions.

Concerning the definition of “acquiring of payment transactions”, besides the issue raised above about the need to narrow the scope and clarify the definitions of “payment account” and “acquiring of payment transactions”, no comments were provided concerning the relevance of the definition, specifically with regard to the emergence of new acquiring models.

When it comes to the inclusion of AIS within the scope of PSD2, as discussed in the previous section, there are some conflicting views across different types of stakeholders. On one hand, banks argued that there is the need to maintain the overall structure and content of PSD so that it continues to pertain to payment services only, and not to expand it to include further open banking or open finance developments. Moreover, AIS has been implemented according to the PSD2 rules, and scoping them out of PSD2 could result in unnecessary implementation challenges. Furthermore, a national ministry noted that the fact that AIS does

[187] 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

not directly involve fund transfers (or payment transactions as a whole) should not be a reason to remove the services from scope as AIS is often an integral part of the payments' related value chain, not to mention the players behind related services, i.e. ASPSP, PIS, PSP.

However, some PSPs indicate that for TPPs and, in general, FinTech providers, in the long term at least, it would make sense to separate AIS services from PSD2 and potentially placing access to account data under the scope of a new Open Finance framework. As argued by a PSP, there is little reason for treating payment data different to, for instance, health data insofar as the purpose for the data sharing is consented to by the data holder. Moreover, the decoupling of AIS from PSD2 may also remove AIS services from the scope of AML legislation, which currently places a disproportionate compliance burden on AIS providers.

Considering the definition of payment instruments, several PSPs also argued that the definition of a payment instrument should also be clarified. One PSP in particular argued that the CJEU case DenizBank AG v *Verein für Konsumenteninformation* case.[188] has led to unclarity and confusion among market actors over the definition of what a payment instrument is, the application of SCA rules and the division of liability for unauthorised payments. The PSP disagreed with the decision made by the court making contactless payment with a card a separate instrument to card payments using a PIN and that are not contactless. It is considered that contactless and non-contactless are different means of communication between the terminal and the chip-card and should not be considered a different payment instrument. They also disagree with the decision that a contactless payment made without a pin is considered as an anonymous payment. This is because the card is tied to an individual and the transactions charged to the individual's bank account.

It was added by this PSP that the decision addresses cards in the physical POS, but the decision also applies to services that are exempted from SCA in the RTS. Considering exempted transactions, they are not subject to SCA until an upper threshold is reached. After passing the threshold, the transactions are subject to SCA. The PSP noted, however, that if card payments are performed contactless, and non-contactless can be considered different payment instruments, it is unclear whether SCA has to be performed for both forms of payment after the threshold has been met. It was also added by this PSP that such checks unnecessarily raise scepticism on contactless payments among consumers even though there is little fraud in such payments.

On the matter of whether the definitions of "payment initiation services" and "account information services" are still valid considering new business models, several TPPs noted that the definition of AIS currently in PSD2 is fairly narrow in comparison to the larger possibility of services that are offered in the market which can also stifle innovation. Consequently, these TPPs argued that the scope of services – as set out in the definition – that could be offered by an AISP should not be limited to presenting 'consolidated' payment account information back to the payment service user. Access to payment account data and the services provided to the customers should instead encompass all areas for which the customer has provided explicit consent for to the AISP. While such insights were provided on AIS, stakeholders did not mention such possibilities for PIS. It should be noted that Commission is preparing an 'open finance framework' initiative which, in line with this suggestion, seeks to enable more data sharing and third-party access to a wider set of financial

[188] Judgment of the Court (First Chamber) of 11 November 2020. DenizBank AG v Verein für Konsumenteninformation. Request for a preliminary ruling from the Oberster Gerichtshof. Reference for a preliminary ruling – Consumer protection – Directive (EU) 2015/2366 – Payment services in the internal market – Article 4(14) – Concept of 'payment instrument' – Personalised multifunctional bank cards – Near-field communication (NFC) functionality – Article 52(6)(a) and Article 54(1) – Information to be provided to users – Change in the conditions of a framework contract – Tacit consent – Article 63(1)(a) and (b) – Rights and obligations related to payment services – Derogation for low-value payment instruments – Conditions under which applicable – Payment instrument that does not allow its blocking – Payment instrument used anonymously – Limitation of the temporal effects of the judgment. Online: Case C-287/19

information and products. Access would be based on the principle that customers have ownership and the right to control the data that is created for them.[189]

The concept of 'e-money'

There is a debate centered around the definition of e-money on whether it makes sense to have a separate Directive (the Second Electronic Money Directive, or EMD2) regulating this product or whether it would be more beneficial to merge this Directive with a future version of the PSD2.

The vast majority of stakeholders consulted noted that since EMIs in effect appear to be providing the same payment services they agree with proposals to merge EMD2 and PSD2 into one text and add e-money as part of the definitions of a payment service. As indicated in the survey analysis in annex 2, the majority (30 replies of 61) were in favour of e-money being added into the list of payment services. From the remaining 31 stakeholders who answered this question, 23 had no opinion and eight were against this proposal. It has been noted by several stakeholders that users do not percieve a difference between an e-money account and a bank account, both PIs and EMIs are both issuing payment cards, and e-money entities are increasingly acting as providers of payment services. Therefore, as they are used, e-money and payment institutions entail the same risks. Furthermore, as e-money services are increasingly used, and as e-money institutions are increasingly providing what is in effect banking services, some payment service providers have indicated that it may be useful to apply the same customer protection requirements that PSD2 require, on services covered by EMD2. Furthermore, considering that EMIs are increasingly acting like a credit institution, one PSP argued that the regulatory environment as well as the application procedure to obtain a banking licence should include the possibility that e-money institutions may be providing credit.

Similarly, stakeholders have argued that different licences are currently being issued for payment service providers and e-money institutions despite the business models being similar. This can create risks as despite similar operations, EMIs are not required to perform know your customer (KYC) checks to verify client identity. As a consequence, stakeholders agreed with merging the legislation and defining e-money as an additional payment service. Some of the stakeholders that agreed with merging the legislation nonetheless stressed that within new unified legislation, clear distinctions between the financial institutions (credit institutions, EMIs and PIs) should be kept as well as the scalability of own legal requirement and obligations. Furthermore, in this new context, e-money should be defined in a technology neutral way. It was added by one national supervisory authority that the merger would allow for an opportunity to reduce the overall complexity of the legal framework, avoid regulatory arbitrage, ensure technological neutrality, level-playing field and future-proof the legal framework. Unifying the legislation may also have the benefit of applying the same customer protection requirements under PSD2 to the wide range of services offered in relation to e-money (and e-money tokens). While there was some agreement that EMD2 and PSD2 should be merged, it was stressed that definitions of e-money should remain consistent with definitions provided in the MICA regulation.

On a similar note, considering that both EMD2 and PSD2 frequently cover the same concepts, when it comes to implementing EU legislation nationally, the existence of two pieces of legislation can lead to misinterpretations and multiplication of regulatory obligations. This was considered to be especially problematic as regards the definition of "agents" in Article 4(38) of PSD2 and "e-money agents"/"distributors" in Article 3(4) in EMD2). It was noted that in some Member States (such as the Czech Republic, Germany and Slovenia) duplication has been limited as provisions have been defined by introducing a single legal text that transposes both PSD2 and EMD2 into a single national act. In other countries, however, transposition has occurred into several legal texts, which very often lead to problems of interpretation, and inconsistency. For the definition of "e-money" agents, in

[189] European Commission (2022). Open finance framework – enabling data sharing and third party access in the financial sector

Member States where there is a single text, it has been made clear that there are two different types of physical persons (e-money agents and payment services agents). Nevertheless, the text ensures that there is a defined way in which an e-money agent can also provide some of the payment services that are linked to e-money. In the cases involving two texts covering the same concepts for PSD2 and EMD2, it is common that they both use the same name for both kind of agents. There is not a clear distinction between the e-money agents and the payment service agents. It was added by other PSPs that the different transpositions leads to complications for providers active in multiple Member States.

Nonetheless, there was some opposition to this proposal. For example, an association of PSPs argued in favour of treating e-money outside PSD2. According to their interpretation, e-money is defined as a prepaid instrument/value which can be purchased and sold and that is distinguishable from, for example, deposits: e-money is modelled on cash, being a claim against the issuer, and it is intended to function in many instances where an electronic equivalent of cash is required. The association also noted that as e-money is a prepaid instrument, the prudential risks associated with e-money go beyond those of settlement, which is that of immediate payment services, as funds are held by the issuer on an ongoing basis; pending a payment instruction. This is an important distinction that separates immediate payments from those that are prepaid and contemplated to be held on an ongoing basis. Furthermore, another PSP argued that the provision of e-money is distinct compared to other payment services. E-money can be purchased and sold as well as pegged to national currencies at par, with a right to redemption at par, but e-money is not a deposit or a debt instrument which should therefore entail a different legal treatment. This PSP expressed concern that the concept would lose flexibility and specificity if there were a merger of EMD2 and PSD2.

Nonetheless, the same association notes that the use of the e-money product to undertake payment services is shared with all other payment instruments, and these are captured in PSD2. The association further pointed out that risks associated with payment service provision are shared and EMIs comply with these in the same way as do PIs and banks. However, the prudential risks and controls associated with the issuance and redemption of e-money are distinct and consequently the prudential obligations that mitigate these risks merit a distinct framework. In the association's view the main differences between payment institutions and e-money institutions lie in the fact that the e-money instrument itself involves the holding of users' funds on an ongoing basis; whereas other payment products offered by PIs do not involve the ongoing holding of balances on an ongoing basis.

Similarly, other stakeholders agreed that despite similar treatment, particularly from the perspective of users, specificities of the products suggest a need for different legislation. The PSP agreed that today all forms of e-money activity are treated in the same way, even though e-money covers a broad range of activities including pre-paid cards and vouchers, online and mobile wallets, and e-money tokens, but stressed that they all have different associated risks. A greater delineation of the different types of e-money activities, keeping a separate legal treatment under different directives, would allow for specific, targeted regulatory treatment for each. This could allow the pertinent regulatory and market risks applicable to each activity to be addressed, including from a consumer protection and financial crime perspective. Such clear categorisation of e-money activities would also allow for a greater level of activity-based disclosures and disclaimers and would accordingly assist with transparency and risk awareness from a consumer perspective.

In either case, banks argue that the concept and the way to regulate e-money may warrant a review. One banking association observed that EMIs have been growing in size with pan-European presence and offering basic day-to-day banking services (a card linked to an account, payments, etc.): thus it is necessary to ensure customer funds protection in these areas as well. Today, many e-money account holders may not be sufficiently informed about the difference between a bank account and an e-money account. A payment institution can in theory provide payment services without ever holding customer funds at the end of its business

day. In other cases, a payment institution can maintain payment accounts which are similar to e-money accounts. A modified regime should treat these two cases in a different manner based on such criteria. Similarly, EMIs that emulate full banking services and whose size exceeds certain thresholds, should operate under a different regime on the principle of “same services, same risks, same rules and supervision”.

On whether the concept of e-money is still fit for the future, some stakeholders indicated that the emergence of new products from (including wallets, as well as virtual and digital currencies) may point to the need to reconsider the concept. It was argued, for example, by one national ministry that the concept of e-money is tailored to smaller card systems and not cryptocurrencies where there is more risk. There is hence a need for EMD2 (or a merged legislation with PSD2) to consider the risks that global e-money schemes could have on financial stability, issues that were not explored in the drafting of PSD2. One PSP specified that legislation should not be prescriptive and be written in a more general manner and include references to the fact that the services may evolve beyond the way they are defined in the current legislation.

Other stakeholders highlighted that e-money tokens (or asset tokens) are not considered e-money under PSD2 or MICA despite there being little difference between the two in practice. Relatedly, another national ministry indicated that there is uncertainty about whether the concept of e-money includes tokens as well as micropayments. Some stakeholders have argued therefore that the concept should include tokens, with one PSP noting that this is necessary considering the likely growth of blockchain embedded e-money products. Such products need to be regulated for cyber-security and customer protection. The case of Poland has been highlighted as an example of legislative uncertainty created by the absence of e-money tokens in the concept of e-money. In this case, domestic legislation allows for banks to issue tokens and share them with clients, but it is not clear whether such tokens can be transferred to other clients from another bank (due to AML requirements). Taking these issues together, stakeholders pointed out that additional requirements concerning the issuers of e-money tokens should be included in legislation, including if EMD2 is merged with PSD2 into new legislation. This can involve incorporating tokens into the definition of funds under PSD2.

Another issue raised was the extent to which e-money products fell under PSD2 legislation. One national ministry argued that unlike other concepts such as a payment account, there is no regulatory definition for an e-money account in PSD2 which creates issues in interpreting and applying legislation. There is for example uncertainty about whether an account combined with a prepaid card with an IBAN number can be defined as an electronic money account or a payment account.

Impact of recent CJEU case law

Very limited evidence has been gathered so far on this topic. However, two elements that were raised by some interviewees are related to the definition of ‘payment accounts’ and ‘payment instruments’. In particular, a PSP association noted that the revision of PSD2 should take into account the interpretation in the CJEU ruling in *Bundeskammer für Arbeiter und Angestellte* vs. ING-DiBa Direktbank Austria (Case C-191/17), where it was held that (taking into account the definition of a ‘payment account’ under the Payment Accounts Directive 2014/92/EU): (i) "the possibility of making payment transactions to a third party from an account or of benefiting from such transactions carried out by a third party is a defining feature of the concept of ‘payment account’"; and (ii) "An account from which such payment transactions cannot be made directly, but for which use of an intermediary account is necessary, cannot therefore be regarded as being a ‘payment account’". Nonetheless differences in Member State interpretation of accounts falling within ‘payment account’ definition has led to difficulties for TPPs active in multiple countries, who may be able to access certain types of accounts in some but not other EEA countries.

Moreover, a national ministry noted that, as discussed earlier, judgments in cases such as the CJEU DenizBank AG v *Verein für Konsumenteninformation* case[190] indicate that there are existing doubts related to the correct understanding of the definitions of a "payment instrument". These doubts should contribute to further discussions on clarifying the existing PSD2 provisions, especially in the context of providers' liability for unauthorised payment transactions.

5.2.5. Licensing of payment institutions

Regarding supervision and licensing, **national competent authorities (NCA) play a central role and may take actions on a risk-based approach.** They could include instructing or warning ASPSPs or requiring amendments on ASPSP rules, procedures and systems (EBA, 2021c).

As noted by previous reports, PSD2 had the greatest impact on firms already operating in the market but were forced to obtain a licence in order to continue operating and be compliant with legal requirements (Polasik et al., 2020).

For the majority of stakeholders consulted, the requirements set out in the licensing regime are adequate. Many stakeholders emphasised that the current licensing requirements strike the right balance between, on the one hand, financial stability and consumer protection and, on the other hand, accelerating market take-up of open banking and market players developing innovative open banking solutions. Most stakeholder interviews do not see a need for any changes to the licensing regime. Survey responses provide a similar picture: licensing requirements are not an issue for the majority of the respondents, while 32 had no opinion or were unaware of any administrative burdens or obstacles regarding licensing requirements.

However, some survey respondents (20 participants) and stakeholders did voice a concern that licensing requirements are disproportionate. To ETTPA, the cost and overhead of PSD2 licensing is significant. They emphasised that it is particularly disproportionate for AISPs and PISPs in relation to the risk they represent. Some other interviewees also commented that the licensing process is heavy and resource intensive under PSD2, and this is an obstacle for smaller actors, such as small FinTechs and AISPs.

Interviewees provided anecdotal evidence on national divergences in the application of the licensing regime. It was reported that each supervisor has interpreted the registration requirements differently with some Member States providing licences more easily than others and having a lighter touch approach to supervision. It was indicated that Lithuania or Luxembourg for example, have much easier requirements to register, so many companies have applied for a licence there and are passporting in other countries. Companies registered in these countries can reportedly do onboarding of customers or KYC in a much simpler way than in countries with stricter regimes such as Portugal or Poland. One PSP explained that lack of standardisation in licensing processes across the EU is an issue. For example, it was mentioned that the procedure in Sweden is more complicated and costly than in certain other countries, where they did not always get a good response within the 90 days and having to respond to a lot of additional questions that were not always relevant. PISP have additional requirements and documentation that have to be completed. It was also reported that there are different interpretations of e-money and payment institutions across EEA. For example, a company licensed as an e-money institution in the UK was considered a payment institution by the Belgian authorities. Another problem the interviewees mentioned concerns UK PSPs

[190] Judgment of the Court (First Chamber) of 11 November 2020. DenizBank AG v Verein für Konsumenteninformation. Request for a preliminary ruling from the Oberster Gerichtshof. Reference for a preliminary ruling – Consumer protection – Directive (EU) 2015/2366 – Payment services in the internal market – Article 4(14) – Concept of 'payment instrument' – Personalised multifunctional bank cards – Near-field communication (NFC) functionality – Article 52(6)(a) and Article 54(1) – Information to be provided to users – Change in the conditions of a framework contract – Tacit consent – Article 63(1)(a) and (b) – Rights and obligations related to payment services – Derogation for low-value payment instruments – Conditions under which applicable – Payment instrument that does not allow its blocking – Payment instrument used anonymously – Limitation of the temporal effects of the judgment. Online: Case C-287/19

that previously had a licence to operate on the continent, but now no longer do following Brexit. These parties, however, continue to operate on the Continent and claim to be exempted from some of the regulations. This is, however, anecdotal evidence and should be treated with caution.

Some stakeholders suggested that the TSP exemption under Article 3(j) of PSD2 should continue to be available to market players. Many FinTechs that are currently offering open banking solutions are too small to be able to do so efficiently, without the support of TSPs. Narrowing down the TSP exemption under PSD2 is likely to limit the ability of FinTechs to rely on TPPs in the development of their solutions. Besides there are tools that already enable NCAs to exercise control over TSPs, such as the EBA Outsourcing Guidelines.

Some interviewees noted that marketplaces such as Bol.com and Amazon.com are in practice large PSPs that are not required to obtain a licence and abide by PSD2 rules. Such marketplaces facilitate large amount of payments between merchants and consumers, as such the risks are high (for example, risk of insolvency and the consequences this would have for merchants and customers getting their funds as these entities are out of scope of PSD2) and they should therefore be regulated.

A few interviewees highlighted the problems with qualified service providers (QSPs) and their certificates. The certificates are provided for a year, and even though a QSP might lose its licence over the span of that year, the certificate remains valid for a year, preventing the ASPSP from checking whether the QSP still holds a licence. It should be clear once a QSP's licence has expired or been withdrawn instead of relying on a certificate with a one-year validity.

Finally, some stakeholders suggested that capital requirements under PSD2 should be re-examined. According to them, the capital requirements are currently quite simplistic but the sector is getting larger and more complex, and as such there might be merit in re-examining these. The initial capital requirements have not been changed since the adoption of PSD1 and that the evolution of different business models for provision of payment services may require further assessment of their adequacy. For example, some entities have mixed business models and therefore the capital requirements should be adapted. Moreover, requirements differ between payment institutions and e-money institutions even though the services delivered can be similar.

5.2.6. Supervision of Payment Service Providers

This section describes the findings concerning the functioning of supervision over PSPs. Overall, while the PSD2 has led to more supervision over payment institutions and e-money institutions, stakeholders have also highlighted issues encountered with this oversight. Issues raised concerned the lack of efficient supervision which was evidenced by delays ASPSPs faced with receiving a fallback exemption, administrative burden involved in obtaining limited network exclusion status, poor quality APIs not being addressed by supervisors, and different degrees of responsiveness of supervisors in different Member States. Stakeholders also believed there was a lack of cooperation between supervisors evidenced by the fact that requirements of different Member States varied significantly when it came to passporting and the ability to operate in another Member States' jurisdiction.

Supervision of payment service providers including payment institutions

Overall, most market players and authorities consider the supervision of PSPs at EU and MS level to be improving as a result of PSD2 but that there are still significant issues in the supervision of market actors as well as fragmentation in approaches across the Member States. Improvements can be seen compared to the previous regulatory context as, according to several interviewees, national supervisory oversight of the e-money and payments sectors has increased significantly over recent years. National competent authorities are improving their understanding of the market and are increasing the intensity of scrutiny over entities authorised under PSD2. A national bank also noted that part of the success of the

supervisory framework is attributable to the EBA guidelines on authorisation and registration under PSD2.

Nevertheless, ASPSPs and TPPs alike have highlighted deficiencies in supervision. For example, as noted previously, **several TPPs have argued that regulators are struggling to act on deficiencies in APIs, which leads to third parties not being able to provide services regulated by PSD2** as was intended by the objectives of the regulation. Another issue entails the applications for fallback exemptions. One PSP noted that there have been significant delays on the part of NCAs in three Member States (Austria, Czech Republic and Romania) to grant the PSP a fallback exemption, while they received it from six other countries (Bulgaria, Croatia, Germany, Hungary, Italy, Slovakia and Slovenia) in 2019 with the same interface.

Another issue concerning supervision that can arise from the different transposition and application of the LNE across Member States is regulatory arbitrage which may ultimately result in impaired consumer protection and competitive distortions. It was argued by one PSP that **in some Member States there is a lack of enforcement and supervision.** It was indicated that in Croatia, national authorities only supervise the status of a LNE if the company has requested an assessment of their status. Otherwise supervisors do not assess whether products offered by the PSP should or should not be under the scope of LNE. It was noted, for example, that some Member States, such as Germany, have strict regulators but others are not as proactive in investigating whether the application of the LNE is functioning as envisioned. **Another factor highlighted which appears to be affecting the supervision of the LNE is the unclarity of the definition which means it can be hard for supervisors to know which companies fall under the exemption or not.** This ultimately affects the level of protection for consumers under the PSD2 and puts authorised entities at a competitive disadvantage. The exclusion of these activities and service providers from the scope of application of PSD2 might mean the EU's anti-money laundering and countering the financing of terrorism rules ("AML/CFT") are not applied on certain actors in the market.

On questions concerning the supervision of passporting provisions, given the significant burden placed on service providers and competent authorities of submitting and reviewing multiple notifications for payment instruments used across the EEA, it was suggested that the EU consider introducing a system for notifications based on the existing processes for the submission and review of regulatory passport notifications. As with regulated payment service providers that exercise passport rights to provide regulated services across the EEA, it would be in the interests of harmonisation and administrative efficiency for a service provider to submit notifications only to its home Member State competent authority and for that competent authority to take a lead role in reviewing the notification. The home member state competent authority could then notify the competent authorities in other relevant member states. This should ensure better information sharing between competent authorities and would be in keeping with the core principles of the internal market.

Concerning the question on whether supervisory requirements for credit institutions should be extended to payment institutions, it has been possible to collect views only from these latter players. Some of these noted that even if they should not be subject to the same treatment from a legal point of view, standards for regulating credit institutions are sometimes applied to payment institutions that are subsequently expected to comply with these. PIs noted that due to the different nature of business models (accepting government-insured customer deposits, credit extension and maturity transformation) banks are exposed to different risks than non-banks and should therefore be subject to different prudential regulatory requirements. Nevertheless, any decision to extend prudential requirements to PIs should be harmonised at EU level so as to avoid national competent authorities 'front running' measures by applying their own super equivalent standards creating regulatory arbitrage within the Single Market.

Supervisory approaches and collaboration between supervisory bodies and authorities across Member States

Most stakeholders along the value chain noted that, within the context of some macro-issues related to the scope of PSD2 (Section 5.2.3) and some highly debated definitions (Section 5.2.4), supervisory protocols at national and EU level have been effectively established to demarcate the various areas of supervision among supervisors. Some authorities argue, especially for providers operating in multiple countries, **it is rather the variety in interpretations of some elements of the Directive that generate confusion, rather than the supervisory mechanisms across countries.** Though others highlight a possible lack of resources (in comparison to the large market of PSPs) in supervisory bodies as a factor contributing to inadequate supervision.

Stakeholders consulted noted that the knowledge and understanding of supervisors has evolved with the developments of the markets. Even if this holds true for most of the interviewees, several PSPs observe that **the degree of responsiveness and transparency in communications and decisions by national competent authorities in certain Member States is higher than in others.** Timely and clear communication could mitigate possible misunderstandings that arise from different implementation and application of PSD2 provisions across the Member States. It was highlighted for example that some Member States (e.g.,Austria, France, Germany and the Netherlands) are very responsive to queries by PSPs allowing for regular contact. PSPs operating across borders noted that others are not responsive or transparent in providing justifications for their interpretations of PSD2 (examples of such Member States are Finland, Poland and Sweden). This has meant that TPPs as a result have been unable to obtain updates on the status of reported issues concerning ASPSPs blocking access to account information. In the case of Finland, one survey respondent indicated that the supervisor does not publish much of its views on interpretation issues, and the resolution and discussion over regulatory challenges remain only between the supervisor and a particular party being treated with in a case. As such, it is unclear how the supervisor interprets EBA's Q&A responses for each supervised entity. According to this respondent, this makes it difficult for a single actor to have a comprehensive overview of the market and there is also a risk of becoming non-compliant due to lacking information.

Few stakeholders consulted provided insight into the functioning of collaboration between supervisory bodies within a Member State. Supervisory authorities that did provide comments noted that collaboration is effective and occurs through regular meetings to discuss issues arising in the payments market.

Considering whether collaboration between national supervisory authorities functions adequately, most NCAs consulted indicated that while each make their own decisions when it comes to regulating their domestic market, there is strong collaboration following procedures laid out in PSD2 and the relevant RTS. Furthermore, the exchange of information between NCAs functions efficiently and dialogue – for example with the EBA to help harmonise interpretations – works well. On the other hand, one national supervisory authority indicated that when a PSP operates in their Member State via an agent whose headquarters are situated in another Member State, they sometimes face a lack of cooperation from the other Member State for certain regulatory requirements. These include the fact that in the former Member State, the PSP may be required to establish a central contact point for AML purposes. The supervisor noted that they have difficulties cooperating with the home Member State when PSPs are not complying with these requirements. It was suggested that difficulties stem from the absence of clear criteria on how to delineate between the freedom to provide services and the right of establishment, including in cases where services are provided solely online or via agents and distributors.

In order to ease the collaboration and the exchange of information between host competent authorities and home competent authorities, it was suggested by a national supervisor that the directive could introduce the requirement to establish a college of supervisors for

intermediaries performing cross-border activities. Furthermore, considering that the digitalisation of the payment services could make the freedom to provide services (FPS) the most common way to provide services on a cross-border basis, intermediaries operating on a freedom of services basis could have significant impact on the host market. In this regard, it was suggested that the powers of the host competent authority be enhanced where services are provided based on FPS, in particular with respect to reporting and including enforcement powers in case of violation of national laws.

In contrast to the overall positive picture provided by NCAs, some EU associations, as well as a significant portion of PSPs, have the impression that collaboration between supervisory bodies has not been sufficient and that coordination with the EBA only occurs with some NCAs. This impression is gathered from the experience with enforcement and monitoring across Member States which is seen as being inconsistent and not taking into consideration actions taken by other supervisory authorities. It was highlighted by one stakeholder that this made it difficult for TPPs to provide EU-wide services consistently and effectively. Other examples noted by PSPs was the fact that **NCAs are taking different approaches to fallback exemption requirements specified in the RTS** (on this case, it has been highlighted that Sweden is an example where requirements are much stronger than other Member States and that therefore it is very difficult for ASPSPs in Sweden to obtain an exemption from providing a fallback). Different approaches to IBAN registration, passport requirements, what is deemed an acceptable API, what can be considered legitimate screen scraping, how TPPs are supervised, and the sanctions for PISPs and AISPs when in breach of the law have also been highlighted as evidence of a lack of coordination. In the case of APIs, the difference means that PSPs operating across borders will use a standard API but this is sometimes not recognised as appropriate in some Member States.

Few stakeholders consulted provided any insight into whether there is a mechanism ensuring cooperation supervisors of PIs and overseers of payment systems, schemes and instruments. It can be deduced from this finding that no mechanism exists despite the frequent calls from stakeholders for greater cooperation between supervisory authorities, NCAs, and other market actors (detailed above).

On the issue of shareholding, few stakeholders had input to provide. Nevertheless, national ministries and supervisory authorities that did provide opinions on the issue indicated that the provisions are fit for purpose and allow regulators to control the share structure in payment institutions. Others indicated that they were appropriate but may require minor revisions. It was for example recommended by one supervisory authority that an assessment be made as to whether ‘group supervision’ for e-money institutions and payment institutions similar to the Capital Requirements Directive could be required under PSD2. Furthermore, one PSP indicated that they are appropriate but can cause excessive regulatory burden on small firms, particularly considering the small risk they pose. This PSP argued that as businesses reach a certain size, provisions over shareholding are appropriate as there are more significant risks to the financial market. One PSP indicated their disagreement with how provisions regarding shareholding are applied because of the need to register an entity from another Member State with their own supervisory authorities despite the entity having previously been regulated in the Member State of origin.

Concerning the question of whether there has been proper application of provisions regarding public registers, most national ministries and supervisory authorities indicated that the provisions themselves and their application have been appropriate. The national and EBA registries allow supervisors to efficiently verify information regarding payment institutions and agents. For users, it allows them to check whether a payment institution is officially registered and authorised to provide the specified payment services.

Nevertheless, **several national ministries and supervisory authorities indicated that the scope of the data included in the registries could be expanded and registries could be more often made up to date.** It was highlighted by one national ministry that the registry only

allows for a verification of whether the certificate is valid. In this regard, it was argued that the data available about the certification of entities should be extended and be regularly updated along the lifespan of an entity so that the registry can consistently provide up-to-date information about PISP status, domicile, and time it has been providing services. It was indicated by one ministry that the EBA registry and national registry are at times not aligned as the former is not updated instantly following changes to the latter.

Other issues regarded the use of registries with one national ministry indicating that the registers should have a direct impact on Authorisation Centres for eIDAS certificates. For example, once a licence is revoked there should be an instant online eIDAS certificates deactivation process to let the market adapt immediately to the licensing authorities' decisions. Another ministry indicated that the data available on the EBA registry should be exportable.

On the part of PSPs, there were few responses concerning the functioning of the registers. Nevertheless, one PSP indicated that they had issues with national registries and how identity verification firms made use of the EBA registry. These issues concerned onboarding and the eIDAS certificate. The PSP in question had a credit institution licence which granted the right to provide cross-border services, including AIS and PIS by their home country competent authority, but they were nonetheless not always listed in the national registries in which they were operating. Furthermore, the PSP was not listed as a PI in EBA registries, but as credit institution (the PSP provides pay as you go service). On the other hand, certificate validation services such as PRETA (firm involved in identity verification) did not recognise the PSP as a TPP as they only based their information on the EBA's payments institutions registry. The PSP indicated that this issue specific to how PRETA performs identify verification meant that ASPSPs did not allow the payment institution to onboard their PSD2 APIs with valid certificates. Furthermore, it was highlighted that the German competent authority did not publish passporting information in its national register, meaning that the PRETA registry did not accurately present the information to ASPSPs using their service to validate certificate information. The PSP had to rely on contacting individual ASPSPs to resolve the situation but others refused to override their automatic system that validated the certificates based on registries.

It was added that some ASPSPs also checked if the certificate was issued by a Qualified Trusted Services Provider. In certain cases, their certificates would get rejected by the ASPSP if the ASPSP's list of certificate users did not include the Qualified Trusted Services Provider that the PSP relied upon. In some cases, ASPSPs' list of certificate issuers were not updated in a timely manner which would cause these certificates' rejections from the ASPSPs' side.

Appropriateness of accounting and statutory audit provisions

Evidence on the appropriateness of accounting and statutory audit provisions is very scarce. In addition to few responses from interviewees, the 35 organisations surveyed (of the 60 in total) had no opinion as to whether accounting and statutory audit provisions are still appropriate. This was followed by the nine companies that argued that they are appropriate but only to some extent. More specifically, only two participants viewed that accounting and statutory audit provisions are not appropriate at all, while seven respondents oppositely viewed that they are is fully adequate.

Nevertheless, of the national supervisors and national ministries that noted that accounting and statutory audit provisions are appropriate and appropriately regulate both PSPs and EMIs, they also indicated that there is currently there is no need for special audit provisions to address the specific business models in the field of payments. However, a PSP noted that PSPs are required by the implementation of PSD2 provisions to have audits undertaken around their SCA compliance and on the use of SCA exemptions. Some professional services firms have suggested that PSPs provide something akin to a gap analysis/compliance review with a law firm instead to meet this requirement, as opposed to a fully-fledged audit. There hence may be merit in the review of PSD2 considering the expansion of the manner in which the SCA and transaction risk analysis audit requirements may be satisfied, as currently

specified in article 3 of the RTS, and in considering whether there is scope for meeting the audit/testing requirements through other means than traditional accounting/statutory audit provisions.

One EU association and several PSPs argued that the accounting and statutory audit requirements should be proportional to the size of the entities involved. This is particularly the case for start-ups for which stakeholders indicated that there should be lowered barriers for entry to promote innovation. Thresholds based on size as well as temporary regulatory sandboxes for start-ups and SMEs were proposed as measures that to promote the entry of new actors into the market and allow them to verify their market fit.

Use of the possibility of granting credit and conducting other business activities by payment institutions

Although evidence is still very limited at this stage, there are some countries (e.g., Poland) seeing a growth of credit activities being performed by PIs. Klarna is one of the most frequently mentioned FinTech players providing services such as Buy-Now-Pay-Later and e-invoicing. However, in the area of granting credit, quoting the words of a PSP the principle of "the same activity creating the same risks should be regulated in the same way" is not currently respected owing to divergent national laws. Thus, this PSP encouraged the harmonisation of permissions across Member States.

EU-passport regime

Overall, payment institutions indicated that the passport regime works well in that it has allowed for the possibility of providing services across the EU. Nonetheless, there are significant differences in implementation across Member States which create obstacles and administrative burden which are seen to impact the effectiveness of the regime. **Ministries and national supervisors note that some authorities require additional notification once the services are launched in the specific country and some Member States have their own policy according to which the passporting is not sufficient if the service is directed to their domestic countries (e.g., the service in available in their language) and requires establishing a branch or an agent.** The ultimate outcome is that a PSP cannot rely solely on the passporting regime but has to check all the specific and domestic requirements in each Member State which is inefficient and costly. National ministries note that, as a consequence, the cross-border provision of services by foreign PSPs is not uniform in all Member States.

Some stakeholders holding exemptions noted that they were not able to passport this status across the EU. One EU association for example noted that despite efforts by the EBA such as the issuing of Guidelines on the Limited Network Exclusion. Such differences also create legal uncertainty for service providers. Diverges exist in the timelines, details that service providers are required to provide as part of the activity description as well as the frequency of the submissions required in the various Member States. Application forms vary from short and standardised ones paired with prompt reactions from the responsible competent authority to very burdensome ones that require the continuous submission of information over an extended period of time. It was nonetheless noted by experts that LNE does not benefit from rules on passporting.

Taking the example of the limited network exemption, market participants note that different interpretations mean difficulties in operating across the EU with an exempted payment instrument. It also adversely affects users who become uncertain as to what extent an instrument can be used in individual EU countries. In the case of fuel cards, difficulties are evident as drivers will use them in numerous countries crossing borders, but they may find they cannot use them for toll charges or roadside assistance in some Member States.

Facing such a situation, this EU association argued that notification requirements as specified in Article 37 (2) should be harmonised to create a level playing field within the internal market. More information exchange between NCAs was also seen as a solution

to promoting more harmonisation and establishing a level playing field. Furthermore, it has been suggested that a service provider should only submit notifications to its home Member State competent authority and for that competent authority to take a lead role in reviewing the notification (including where this relates to the use of payment instruments under the limited network exclusion in other Member States). The home Member State competent authority could then notify the competent authorities in other relevant Member States. This was seen as ensuring better information sharing between competent authorities and would be in keeping with the core principles of the internal market. In addition, it was also argued that the notification procedures should be standardised (if not made identical) with respect to format and scope of information that should be required.

In February 2022, the EBA published guidelines on the LNE under PSD2 which indicated that their own assessment of queries about the application of the exclusion has led it to similar conclusions discussed by stakeholders above. The EBA agrees that implementation and application of the LNE provisions differ greatly across Member States and that this hinders the goal of establishing a Single Market for payment services and allows for regulatory arbitrage. The EBA therefore indicated that it intends to publish guidelines with the intention to converge Member States' practices in this regard. It notes that such guidance will cover "*inter alia*, the use of payment instruments within a limited network, the criteria and indicators to qualify a limited network of service providers or a limited range of goods and services as such, the application of the LNE by regulated entities, the notification requirements and others."[191]

Furthermore, considering the significant burden also placed on national competent authorities of reviewing multiple notifications for payment instruments used across the EEA, the previously mentioned EU association suggested that a central system for notifications be introduced which would be based on the existing processes for the submission and review of regulatory passport notifications. Another PSP argued that a single website detailing the requirements for providing services in each Member State would help with promoting compliance on the part of service providers.

Some entities consulted that are considering launching operations in other Member States noted that they are aware that PSD2 is a Directive and not a Regulation though suggested their preference for it having been the latter. They noted that in the case of passporting, a Regulation would have allowed for more harmonisation across Member States in the regulatory requirements imposed on payment institutions seeking to operate in Member States other than their host jurisdiction. In this regard, transposition would not lead to such divergences whereby some Member States take more restrictive approaches compared to the requirements of the current directive and others have laxer requirements. Nevertheless, recognising that it is currently a directive, they noted that it would be beneficial to foster some convergence between such Member States. One national supervisor argued that the current situation makes it difficult for regulators to keep an overview of activities in their market when firms from 'laxer' jurisdictions passport to 'stricter' markets. This national supervisor noted that it would be beneficial to have a database in which market parties list their activity per Member State (e.g., in terms of revenues or customer base) so that domestic supervisors can monitor the activity in their markets even when a firm is not licensed by them. The supervisor pointed out that it is a risk that passporting firms cannot be monitored to the same extent as parties licensed in their domestic market. Several PSPs noted that France has particularly burdensome requirements for a PSP to establish themselves in this jurisdiction, and that several have therefore registered in Luxembourg and Belgium where restrictions are laxer.

Moreover, it was noted by one PSP that in some Member States, local regulations assign to NCAs the powers to supervise and intervene in the activities of licenced PSPs from other Member States providing their services on the cross-border basis. This includes restrictive measures before providing a notification to a home Member State. This has been found to be particularly the case when a PSP uses an agent or e-money agent/distributor. This PSP

[191] EBA. (2022). Final Report: Guidelines on the limited network exclusion under PSD2

indicated that supervisory overreach could be acceptable for consumer protection purposes but not when it comes to checking licensing requirements (as these are established in the host Member State). The impact is that PSPs face uncertainty and additional costs of hiring local consultants to verify their compliance with local laws despite having the right to passport their licence. It was argued that clearer provisions in PSD2 in regards to the supervision, is needed especially for PSPs offering their services on cross-border basis. This should take into consideration the difference between the right of establishment and the freedom to provide services, but also the country-of-origin principle.

One PSP indicated that these issues have also been stressed by the EBA's Report on potential impediments to the cross-border provision of banking and payment services of 29 October 2019. The EBA notes that there is a lack of a clear set and up-to-date criteria/guidance or Level 1 rules for determining the location of the provision of financial services (including payment services), i.e. whether such services are being provided cross border. This is important because the passport notification (either to provide services on a 'freedom to provide services' basis or a 'freedom of establishment' basis) and, consequently, the extent of host State supervision, only apply when services are being carried out cross-border. The lack of clarity is particularly acute with regards to services provided via digital means, e.g., via internet or apps, and has been identified in the EBA's Report as an issue faced by institutions, including new entrant FinTech firms.

PSD2 waiver for small payment institutions (article 32)

On the basis of national legal research, section 4.5 above indicated that in practice, the application of the exemption under Article 32 in Member States legal systems has led to the introduction of special licensing regimes for small PIs. This included the establishment of dedicated entities. Examples were provided in the above section including for Belgium, where our findings have found that a light regime for limited payment institutions and limited e-money institutions has been put in place. Other cases include Lithuania where payment institutions may licence for the provision a restricted set of services but cannot provide such services in other Member States.

As noted above, the evidence indicates that the introduction of special regimes has not appeared to have affected the level playing field and special regimes do not appear to hinder access to the market. The market for payment services does not at this stage have a large amount of small payment institutions. Nevertheless, evidence highlighted above indicates that should the threshold be raised (because of inflation or growth in the volume of online payments by small payment institutions), this could be beneficial for small PSPs, particularly those close to the threshold and would need to request a full-scale licence as a result. This was deemed to be the case as such entities could save costs and time needed for the obligatory licensing proceedings for small payment institutions upgrading to the status of a standard payment institution. Furthermore, it would make them more competitive against standard payment institutions. The previous section therefore argued that the threshold is appropriate under market conditions though an increase could provide benefits to small payment institutions and allow for greater competition. These issues are further elaborated on in section 4.5.

Nevertheless, on the basis of interviews and survey responses of payment institutions and national authorities, little evidence was gathered on these questions as stakeholders largely did not have awareness or an opinion on these questions. Considering the survey responses, 33 out of the 60 answers had no opinion or were unaware of the topic. This was followed by nine participants who believed that PSD2 waiver and the accompanying notification requirements upon payment institutions is adequate but only to a small extent as well as only eight respondents who in contrast viewed that the PSD2 waiver and notification requirements are adequate.

From the few interview responses, the overall trend seems to suggest that, in line with the national legal research, in some countries this waiver was either not made available or not

used by small PIs: in one case, an interviewee flagged a lack of information on this possibility, in another case, an interviewee noted that it was a deliberate choice to adapt their technology to the regulation rather than start to grow outside the scope of PSD2 to then have the need to reinvest in compliance to adapt to the requirements of the Directive. The only remarkable exception has been reported in the Netherlands, where the national supervisor noted that this waiver is commonly used by small payment institutions.

5.2.7. Transparency of conditions and information requirements

This section provides evidence on the clarity and effectiveness of conditions and information requirements of PSD2. It will also assess whether these requirements facilitate customers' choice. The findings below indicate that stakeholders believe there is an excess of legal and technical information which make it difficult for consumers to understand the services they are using. Relatedly, TPPs and ASPSPs believe that they are required to provide too much information which is not seen as useful for consumers.

User convenience, choice and understanding of payment products

Overall, there is consensus across the different categories of stakeholders that the PSD2 requirements ensure an adequate level of transparency and information for payment service users and they are in line with the aims of protecting consumers. They are therefore necessary provisions. **However, as noted by the majority of PSPs and national supervisors, its effectiveness is limited by an excess of legal and technical information received by private clients (beyond their interest which tends to just be the operational functioning of the service and the impact on their daily usage).** This can make it difficult for them to identify the essential characteristics of payment services, both in the pre-contractual phase and in the execution of the contract. One EU association suggested that the essential information can be composed of the name of the PSP, type of contract and term, main fees and interest rates, contact options. Furthermore, because of the excessive amount of technical information that users do not read, risks involved in these services are not fully grasped by them. Similarly, as users are unable to perceive the differences between the payment services and instruments available, they are unable to make comparisons, preventing any intended increase in competition in the market.

The information contract requirements, framework services contracts and single service payment contracts are in some cases redundant and do not facilitate a good understanding on the part of consumers over the services they are using. Therefore, several stakeholders consulted have indicated that **new legislation should remove overlaps in responsibilities over transparency requirements and simplify disclosure obligations.** It was indicated, for example, that when a PISP is involved in an e-commerce payment, both the PISP and the bank have to provide information to the consumer which is seen as being excessive and beyond the interest of a consumer. Similarly, another EU association indicated that AISPs often find they must provide the statements to their PSUs which duplicate what they are receiving from their ASPSP.

Several ASPSPs were of the opinion that consumers do not have a good understanding of data which they are allowing access to as well as how this data is being used (and potentially monetised). Consumers are, for example, often unaware that their payment data is being used to offer them more targeted products or services. Therefore, it was their opinion that consumers are too often providing permissions of access. Furthermore, it has been stressed by several stakeholders that despite the information and transparency requirements, consumers still do not have a full understanding on what open banking is, the implications of their involvement, and the specificities of the different players involved in the market i.e. PSP, PISP and AISP etc.

As a proposed solution to the lack of understanding and the overload of information, PSPs and national supervisors argued that **requirements should induce market actors to provide the essential information on the payment services provided (both in the pre-contractual and**

contractual stages). In addition to condensing the amount of information provided, which could facilitate understanding, it would allow for comparisons between services. One EU association highlighted that the provision of information should follow a 'push and pull' model. The 'pull' refers to the situation in which a user requests and subsequently receives specific information. The 'push' situation involves information being sent in anticipation of a user's needs or the initial information package includes information not specifically requested.[192] Applied to this context, the 'push-information' could entail (in addition to essential information), the initial information package indicating to PSUs where further information is available. All other information (e.g., information on dispute resolution, supervisory authority) should be made available to the payment service user, e.g., via the PSPs' website ('pull-information') but not included in the information package.

Application of transparency and information requirements by courts

One PSP has highlighted a discrepancy between the way information and transparency requirements are described in PSD2 and how they have been interpreted by the German Federal Court. Article 54 of PSD2 indicates that when PSPs propose to make changes to a framework contract or the information and conditions specified in article 52, the PSP is required to notify the PSU in paper format of the changes. This must occur no later than two months prior to the proposed implementation. If the PSU does not notify the PSP of their acceptance or rejection of the changes, the PSP must inform the PSU is assumed to have accepted the conditions. On the other hand, the German Federal Court has rejected the notion that a user has accepted the changes if it does not notify the PSP of either a rejection or an acceptance of the conditions. The federal court specifies that active consent needs to be provided for changes in the conditions to be regarded as accepted. The PSP argued that this creates significant barriers in obtaining consent for their services to be implemented.

Need for additional rules

Supervisors and national ministries consulted, however, flagged the need for some additional rules for the purpose of user security and for consumers to make more informed choices:

- The inclusion in the contractual information of questions related to security and clearer definitions of what is understood as "authorised operation" and of the forms of use of payment instruments. In general, especially in relation to complex terms, examples could be added.
- Mandatory establishment in the contracts of the limits of disposition through payment instruments.
- Obligation of a disclaimer on all websites and payment gateways in which the IBAN is used to confirm that it is clear to the user that payment service providers do not check IBAN/holder. Such a disclaimer can ask the consumer for example to "confirm that the IBAN corresponds to the one indicated by the recipient of the payment" as PSPs do not compare ownership and IBAN.
- Possibility of precautionary blocking by the payment service provider of the beneficiary who receives supposedly fraudulent operations in an account (though the legal implications of such a possibility was not discussed).
- A prohibition on PSPs to be able to unilaterally raise the limit of a payment instrument (the money that you can pay or retrieve in cash) previously chosen by the consumer and a mandatory establishment in the contracts of those limits.
- A notification requirement from the payer institution to the user prior to the execution of a payment transaction (especially in the case of direct debits, recurring payments, and MITs) and when a new mandate has been established. This could help enhance the protection of users who may not be aware that merchants have a mandate to initiate payment transactions from their account (which can be fraudulent).

[192] Cybenko, George., Brewington, Brian. (1999). The Foundations of Information Push and Pull. *The Mathematics of Information Coding, Extraction and Distribution.*

- With regards to instant payments, rules to impose transparency obligations on PSPs making use of such payments. For example, article 80 could be amended to state that the PSU should be made aware that an instant payment cannot be revoked within the usual time for revocation of other payment services.

Furthermore, one supervisor added that in the case of unregulated entities that use authorised entities to be able to offer their customers payment services in such a way that (i) the unregulated company is the one that deals with users and (ii) the entity of payment adapts its services so that the non-regulated entity develops its business model, the following measures could be incorporated:

- Clarify who is ultimately responsible for the information obligations to the user when the services are provided through unregulated FinTech intermediaries;
- Clarify the responsibilities and obligations of the regulated payment service provider when it provides transfer services to digital platforms (i.e. marketplaces or crowdfunding platforms). This is because in these cases there is a chain of intermediaries between the end user and the payment service provider, whose respective responsibilities should be clarified.

PSPs, on the other hand, have argued on different occasions that additional rules are not necessary as they do not want to exacerbate the overload of information already provided to the user.

Should (differentiated) transparency requirements be considered for account statements?

Very few stakeholders consulted provided feedback on this issue and several that did comment either did so vaguely or noted that this topic was not a priority issue for them.

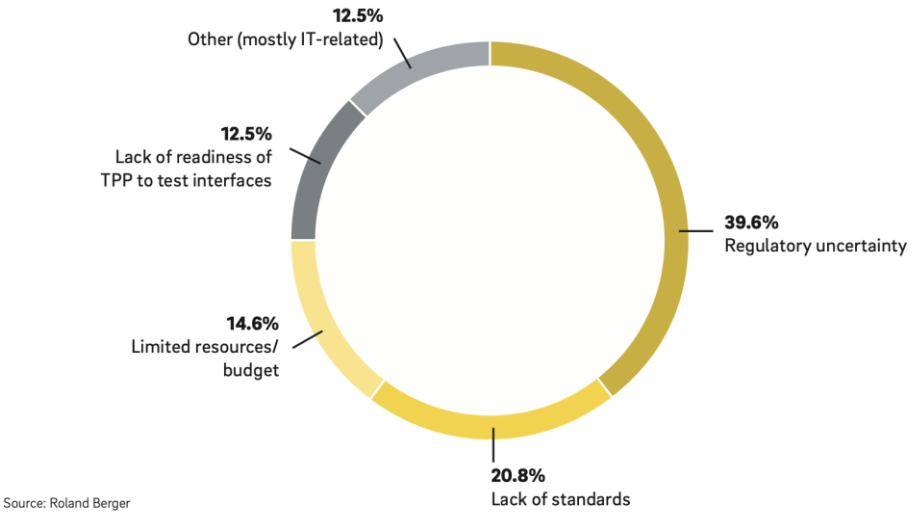
5.2.8. Strong Customer Authentication (SCA)

SCA was introduced as a core component of PSD2 with the objectives of (i) enhancing consumer protection against the risk of fraud (ii) promoting innovation and (iii) improving the security of payment services across the EU[193]. SCA requires the use of multi-factor authentication (MFA) to confirm customer identity when a payment is initiated by them. At least two of the following three categories are required for SCA: knowledge (password or PIN), possession (phone or physical token) and inherence (fingerprints or face recognition). The RTS on SCA[194] define specific requirements to ensure secure authentication and communication between different actors of the payment ecosystem.

SCA implementation was complex, challenging and significantly delayed. The EBA originally planned for SCA to be enforced throughout the EEA by 14 September 2019, but due to a general lack of market readiness (see figure below) and lack of clarity on the underlying standards, Member States were given additional time until 31 December 2020 (unless a national ramp-up plan was agreed). Interviewed industry stakeholders reported that the overall delay in implementation of SCA, as well as the publication of additional standards and multiple opinions by EBA (often quickly outdated in their view, and many not legally binding) created legal uncertainty, complexity and implementation challenges. In the words of one PSP interviewed: “Sometimes PSPs have expended time, effort and costs in understanding, preparing for and implementing solutions compliant with regulatory technical standards that became outdated in very short period.” Some stakeholders also complained that EBA standards were published “too late” and “were developed unilaterally” without adequate stakeholder consultation.

[193] These objectives are spelled out in the Regulatory Technical Standards on strong customer authentication and secure communication under PSD2 published by EBA.
[194] Op cit

Figure 13: Challenges in implementing SCA



Source: Roland Berger (2019) Adapt or die? Why PSD2 has so far failed to unlock the potential of Open Banking. Based on a survey of representatives from more than 40 leading banks and TPPs in 12 EU markets (Germany, Austria, Sweden, Denmark, Finland, Norway, Portugal, Italy, Spain, France, Netherlands and Belgium).

Industry stakeholders highlighted a range of obstacles and challenges in the implementation of SCA. These include:

Divergent national ramp-up schedules and approaches to implementation and enforcement, which have resulted in variations in processing capabilities and application of risk-based authentication, thus increasing operational complexity for European online businesses that are increasingly cross border in nature.

Complexity of initiation of payment transactions applying SCA due to more complex integration as well as the complex optimisation processes included in the decisioning systems. The introduction of SCA has required all entities within the payments value chain to make changes on how they process a payment transaction as PSD2 requires authentication to be completed prior to funds authorisation. To meet this requirement, merchants have had to, for example, develop appropriate authentication strategies including supporting 3DS for card transactions[195], updating their analytics and transaction tagging; gateways had to upgrade their service to the new EMV 3DS2 standards for card transactions; acquirers needed to manage exemptions and fraud rates; networks have had to update rules, directory servers and provide communications to all parties; and issuers needed to authenticate PSUs, apply exemptions, improve the performance of their 3DS2 messaging protocols and enhance their risk controls.

The technology that is being mostly adopted to achieve SCA compliance for card transactions is called 3D Secure (3DS) . This international standard is developed under the auspices of EMVCo and called EMV 3DS (or 3DS2). It is an updated version of 3DS1 which was introduced in 2000 under the network brand names Verified by Visa, Mastercard SecureCode and American Express SafeKey. 3DS1 is SCA-compliant, but due to the higher transaction fees being applied by Mastercard for 3DS2 (as compared to the older version, 3DS1) and announcements of it being made will reach its 'end of life' in October 2022 and many merchants have moved or are moving to EMV 3DS2.1. EMV2.2 introduces additional exemption opportunities and is widely available from issuers. The standards continue to evolve with the

[195] E-wallets and other local payment methods (e.g. Bancontact Mobile in Belgium, iDEAL in The Netherlands, MobilePay, Vipps and Swish in Norway, Sweden, Denmark, and Finland) often provide their own SCA-compliant authentication. For example, card-based payment methods such as Apple Pay or Google Pay already support payment flows with a built-in layer of authentication (biometric or password). SCA does applies to PayPal only if the customer has a credit card on file for them. iDeal, Giropay and Sofort, require the payers to pay via their bank account through their online banking access. These credit transfers and invoice solutions such as Klarna also already meet SCA requirements.

recently released v2.3 specifications including support for games consoles, Internet of Things (IoT) .

Several industry actors complained that due to the EBA technical guidelines, the card payment ecosystem has been forced to adopt 3DS solutions despite the suboptimal user experience and 3DS not being the most effective approach to all payment use cases and risk models. They argue that, instead of promoting competition, PSD2 has de facto, resulted in 3DS becoming the default and dominant approach for card transactions. Moreover, it was reported that in some countries regulators asked the banks to prioritise the implementation of EMV3DS, thus undermining one of the objectives of the PSD2 which was to promote competition. One stakeholder claimed that 3DS mostly benefits large card payment networks as they earn a click-on per transaction. Everything that goes through 3DS is billable as per network rules even if there is no SCA. As an example, for some low value transactions 3DS calls paid to ICS networks may cost more to the merchant than interchange fees. Regulators pushing for all transactions to be done through 3-D Secure thus affects competition.

It was reported that application of SCA has been technically challenging where there has been a need to migrate from legacy systems to a new platform. Specific challenges cited by issuers were: relying only on strong factors, replacing static passwords with dynamic authentication; implementing exemptions, especially TRA where risk-based logics are required, including fraud rate calculation and advanced reporting; implementing proper fallback methods (when primary authentication solution is not available); having better insights on what happens before the payment transactions are initiated and if the SCA exemption is justified when it is it being applied by the merchant; reducing and then eliminating non-compliant transactions.

Merchants strongly rely on their PSP/acquirer and/or payment gateway provider to implement an SCA solution which also means that in some cases they need to develop new logics, migrate to new platforms, or wait until their PSP makes necessary development on their side. These issues could lead to incorrect implementations resulting in poor authentication experience, non-compliant transactions or continuous technical failures. It is also important to support the ability to correctly respond when a card issuer PSP is requesting SCA (in the same session).

One of the stakeholders interviewed explained that EMV 3DS supports around 100 data points (e.g., payer addresses, payer email, payer phone, payer device information). However, some of these data points are often not provided by merchants because of required platform changes and data privacy concerns. This increases the fraud risk and has been raised as a big concern by many card issuers. Another stakeholder highlighted that the requirement for more data fields under 3DS2 as compared to 3DS1 is leading to incorrect flagging of transactions and misinterpretation of network specifications as each network has different requirements for flagging SCA characteristics.

Challenges with regards to the necessary tools to apply SCA optimally include, for example, the necessity to request approval for using delegated authentication by the merchant from each customers' issuing bank (which is considered impractical by some industry actors and, according to them, prevents implementation of this method to streamline the authentication process).

Significant costs of implementing advanced SCA solutions for payment instruments like cards, to enable 3DS2.1+ protocol and complementary services.

The way SCA is specified in the RTS, as well as the specific requirements on dynamic linking, have pushed PSPs into specific technological solution*s* that are heavily based on devices, and especially the use of SMS OTP (this is anecdotal evidence. There are no hard facts to support this). This has led to significant operational expenditure (with a cost per SMS of around 5 cents in certain markets), while increased the payment sector's dependence on the telecom sector, which in turn has had an impact on the resilience of payment networks.

Technical outages. Interviewed PSPs provided examples of how transactions in Spain and Germany could not be processed for hours due to telecom providers' systems being down. When the SCA infrastructure (card issuer's access control servers, merchant gateways, scheme directory servers) fails, online shops cannot sell. It was pointed out that some countries (e.g., UK) allow payments to continue without SCA during major outages.

RTS being difficult to understand and implement in accordance with the expectations of supervisory authorities.

Inconsistent implementation on App To App flow (also known as universal link flow) which is not standardised or clearly documented. ASPSPs tend to have different SCA approaches for each channel, creating confusion for the PSU. The SCA processes are not optimised and this leads to competitive advantages for card-based transactions compared to app to app transactions.

App based transactions. According to several stakeholders, SCA can be very challenging when the purchase is initiated from a merchant app (or a place other than the browser environment) and the user/cardholder has the banking app on the same device or owns more than one device. When an app-based transaction is taking place, there is a strong need for close collaboration between the merchant and issuer, which reportedly "is not easy to conduct".

Lack of access to richer Operating Software (OS)/device controls (see also sections on scope and data access). Such access is essential for PSPs to offer convenient and secure payment services, especially on mobile devices, and to comply with SCA and fraud prevention rules. Device manufacturers' blocking of such access distorts competition as rival PSPs cannot make use of these technologies, which are exclusively used by OS operators to provide their own payment services.

Policies around cookies, device identifiers, and other device-level data, by some device manufacturers, moreover, make the seamless integration of some payment services within merchant apps challenging (see also section on scope of PSD2). This not only undermines the seamlessness of the SCA experience, but also PSPs' ability to deploy essential counter-fraud measures.

The challenges to making dynamic linking work in practice across a complex ecosystem. One of the PSPs interviewed mentioned that the rules do not sufficiently take into account current customer experience journeys, and merchant needs. For instance, when final amounts are known only on the merchant website, after the customer has already gone through the payment experience (so-called 'over-captures' scenarios). These experiences typically involve the addition of shipping at a later stage in the customer journey. In these cases, the requirements for dynamic linking have been met before the final amount is known, and this only happens on the merchant website, which sits outside the PSP's domain. This type of customer flow is preferred by some merchants as it drives conversion. According to the interviewee, this should remain a merchant choice and rules should avoid limiting such use-cases.

Likewise, the final amounts are often not known to the customer when shopping online from a supermarket (as the price can vary depending on the weight of products such as fruits and vegetables). However, authentication is only done taking one quantity into account. As the amount charged to the customer cannot be higher than the authenticated amount, this issue has resulted in cancellations of transactions and ultimately loss of business for supermarkets interviewed.

Moreover, SCA is impractical to apply in certain contexts and thus cannot offer protection in such instances e.g., for providers offering in-flight Wi-Fi services where the user is not connected to the internet and therefore cannot use any connected devices for 2 factor authentication.

Challenges involved in making use of external SCA capabilities, which would make the customer experience more seamless and convenient. For instance, using external authenticator apps, or governmental eID schemes.

Divergence in SCA approaches across issuers and countries. As SCA authentication decisions are taken by individual issuers, there are many variations in approaches being taken across each of the EEA countries. This has brought additional complexity and confusion to a merchant as they need to support a wide range of authentication approaches and payment flows.

A Recent UK study echoes some of the above issues.

SCA implementation challenges identified in the UK

1) Small/medium size retailers are facing integration difficulties (and increased costs) to deploying SCA compliant solutions that allow the use of payment cards for remote/e-commerce payment transactions. These retailers are dependent on the support of Acquirers and Payment Gateways to deploy SCA-compliant payment solutions. Acquirers and gateways have, however, prioritised the larger e-commerce merchants over SME e-retailers that have limited access to such solutions.
2) Merchants are required to enable the required Java scripts within their local codebase to allow the biometric data collection needed to complete checks during a 3DS session. Not all merchants are aware of this requirement and others have security concerns over enabling Java scripts.
3) The travel and hospitality sector have several specific SCA challenges including the number of intermediaries involved in processing a payment and the reliance on indirect sales channels.
4) In-app payments are trickier to manage than browser payments. Merchants need to work more closely with their payment providers and support the latest version of 3DS to avoid unnecessary declines.
5) Lack of readiness among small merchants due to multiplicity of factors such as lack of awareness, or distraction by other business priorities.
6) Large issuers have faced several issues in order to be SCA-ready. Often these related to constraints from legacy systems operated inhouse or by third party processors. The transition to EMV 3DS by ACS providers took longer than anticipated and was hampered by their international ownership and 3DS not being a core product. Another challenge initially faced by large issuers was the low levels of cardholder mobile phone numbers held on file but, this has improved over time. Newer issuers such as challenger banks (e.g., N26) and FinTechs on the other hand, have found SCA compliance much easier thanks to their modern platforms, lack of legacy systems, stronger IT capabilities and higher mobile banking adoption rates.

Source: The Payments Association (2022) The Long and Winding Road to SCA. UK readiness status and key learnings from Europe

Even today, there continues to be lack of clarity on some aspects of SCA requirements. There is some confusion regarding the application of SCA in case of one-leg transactions (EBA, 2018). Moreover, SCA exemptions are complex and not easy to comprehend (ECB, 2019). According to various interviewees, businesses today are still struggling with the complexities of the rules. For example:

There continues to be confusion over the application of SCA rules in areas such as ‘out of scope’ transactions and off-session payments[196]. Merchants also seem to lack clarity on the fact that in order for the SCA exemption for MITs for recurring payments to apply, the first “on-session” payment initiated by the customer has to be authenticated through two-factor authentication (2FA.) Subsequent recurring transactions after the first authenticated transaction are effectively initiated by the payee (MIT) and therefore out of scope of SCA. MIT was thus highlighted as an unnecessary exemption by some stakeholders, and it was suggested that this exemption be removed from PSD2.

Another set of transactions which requires attention are the MOTO transactions, where confusion has arisen whether MOTO is in or out of scope of the PSD2 SCA requirements. Stakeholders requested that this issue be addressed and clarified. It was highlighted that the EBA held in two Q&As on MOTO and PAN Key entry that card payments (including PAN key

[196] Payments initiated when the customer is not present online, for example, renewals / recurring payments, trial to paid etc are classified as Off session payments. These transactions are also referred to as Merchant-Initiated-Transactions

entry) qualify as 'electronic' transactions and cannot therefore benefit from the MOTO exclusion. The industry representative interviewed disagreed with the EBA's position for the following reasons: (i) the MOTO exclusion was introduced in PSD2 (Recital 95) because of the technological challenges in authenticating when placing an order via phone or mail; (ii) MOTO exclusion was introduced in PSD2 to take into consideration account cards. If the MOTO exclusion does not apply to cards, it is unclear which transactions may benefit from this exclusion.

On the Low Value exemption, the EBA has clarified that the count of these transactions should be done at the payments instrument level (e.g., card) This means that issuers must track the use of this exemption for each card, including the number and the total value of all transactions since the payer was last authenticated via both authentication and authorisation if the exemption is to be applied on both channels. This creates unnecessary extra burden for issuers as it requires them to synchronise the counting process for both channels (authentication and authorisation) which is technically complex. It was suggested that one counter could be used in authorisation and another one in authentication for the payment instrument rather than requiring issuers to synchronise counters of both routes so the two do not have to be synchronised but may count independently of each other.

Interviews suggest that further clarity is needed on the calculation of fraud rates applicable to TRA. TRA exemptions are at the moment taking into account also the acquirer liable fraud. This has resulted in the blocking of certain transactions. It was argued that PSP should only include the fraudulent transactions for which it is solely liable (excluding the fraudulent transactions where another PSP was liable) so that each PSP is incentivised to detect, mitigate, and reduce fraud through the use of their own fraud rates

Currently, a PSP may not participate in the TRA exemption unless its entire portfolio (i.e., all of its merchants in aggregate) meets certain fraud thresholds. It was reported that for a payee PSP (acquirer), this creates a very strong incentive to not serve a diverse set of merchants, but only to serve merchants that have similar fraud profiles to each other. Otherwise, the lower-fraud merchants are penalised by higher-fraud merchants who are using the same PSP. This can distort the payee PSP market over time. It was recommended that payee PSPs be allowed to avail the TRA thresholds on a merchant-by-merchant basis rather than on a portfolio level.

A large issuer also mentioned that the EUR 500 limit for TRA exemption should be reviewed, as it is not necessary if the risk is low. They explained that for high spending groups, this limit is easily reached and as the exemption only applies to low-risk transactions, the limit could be increased to EUR 2000 without compromising security.

With respect to SCA exemption for corporate transactions, a large issuer mentioned that a PI needs the approval of national competent authorities to apply these exemptions. It is the only exemption that needs this approval and this creates regulatory fragmentation and burden. There is no passporting of exemptions, so one could have an opinion of the Belgium national competent authorities on specific products that differs from the opinion the French national competent authorities, for example. Furthermore, several stakeholders called for the need to clarify the definition of corporate exemptions. According to them, the difference between consumer products and corporate product is "very ambiguous" in the definition. This results in corporate products not being considered corporate and thus not benefitting this exception.

Several merchants were critical of the optional nature of the exemptions. According to them, this leads to a situation where issuers are reluctant to implement exemptions for merchants. It was reported that there are very few PSPs that have implemented all the SCA exemptions under PSD2 and that PSPs are systematically failing to respect the use of certain exemptions (they are demanding authentication where the payee's PSP has submitted a transaction requesting the TRA exemption, even where all the requirements are met). It was suggested that the exemptions should be made mandatory and PSPs should not be able to make systematic refusals in case of valid exemptions, especially since the use of exemptions can reduce friction in the payment process and enhance user experience. Specific exemptions

cited in this regard were trusted beneficiaries (whitelist) and secure corporate protocols. Interviews suggest that these remain unclear in the industry and are generally not supported by existing protocols.

It was also highlighted that the EU authorities need to make it clear who is liable for what if they elect to apply exemptions. It was suggested that the party that initiates the exemption should be 100% liable for the exemptions. Furthermore, it would be prudent to clarify in the Directive whether exemptions specified in delegated acts (Art. 98.1.b) are limited to voluntary exemptions, applied by the ASPSP at its own volition (after assessing risks and benefits, both in general and to the PSU) or if it also includes the right to issue mandatory exemptions, in effect issuing prohibitions for applying SCA where the Directive sets forth a mandatory requirement (in absence of an applicable exemption).

Finally, it was suggested by several stakeholders that there should be an exemption for technical outages. Legislation should allow payments in these cases by implementing exemption for outage and having a solid resilience plan under a framework which sets the rules and what kind of additional monitoring would be required.

Stakeholders pointed out that there is uneven transposition and compliance with SCA rules. A few interviewees claimed that certain countries and issuing banks are still not fully compliant with the SCA rules (e.g., server-to-server communications, sometimes companies want to initiate a payment transfer between laptops from an API). Another interviewee (TPP) explained that in France, a technical protocol ("EBICS")[197] can be used without SCA to access accounts or initiate payments. It is claimed that PSD2 does not apply to this protocol because a specific contractual relationship exists between ASPSP and service users. It was also highlighted that TPPs in France cannot initiate batch payments because ASPSPs require beneficiaries accounts to be pre-declared using a direct bank interface, but without providing TPP any means to declare those accounts.

Fraud rates have declined following implementation of SCA, but this does not necessarily imply causation. One major PSP interviewed reported a 40% drop in the number of attacks on their accounts, noting that SCA has made it more difficult for fraudsters to access payment accounts and initiate payment transactions. Several other interviewees also confirmed that fraud levels have declined, although they were not able to provide any figures.

Data compiled by EBA shows that the share of fraud in the total volume and value of *remote card payments* was higher for payments that were not authenticated with SCA as compared to payments authenticated with SCA in H2 2020. For remote card payments reported by issuers, the share of fraud in total volume is five times higher for payments authenticated without SCA compared to the payments authenticated with SCA, and three times in terms of value.

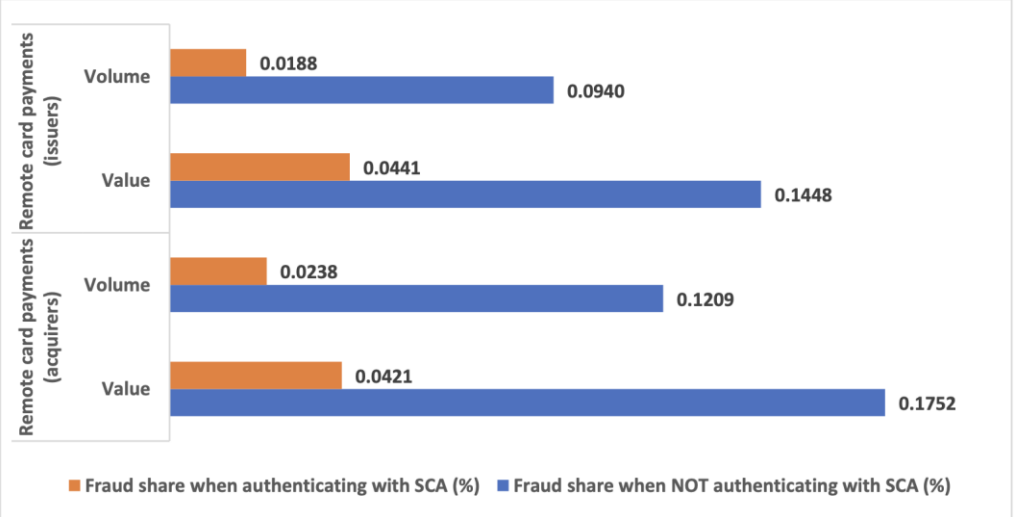
The same pattern was also observed for *non-remote card payments*. For H2 2020, the share of fraud in the total volume of non-remote credit transfers authenticated without SCA was two times higher compared to the share of fraud in the total volume of transactions that are authenticated with SCA (EBA, 2022).

However, in the case of *remote credit transfers*, the fraud rate was higher for payments authenticated with SCA as compared to payments that were not authenticated with SCA in H2 2020, both in terms of volume and value. The EBA offers two potential explanations for this: (i) SCA payments are exposed to a higher risk of fraud, as there are inherently of higher risk than the SCA exempted lower-risk transactions (e.g., low-value payment exemption in Article 16 of the RTS). (ii) the fraudulent credit transfers where SCA was applied might be due to spoofing, authorised push payments and transactions initiated by the account holders after social

[197] EBICS (Electronic Banking Internet Communication Standard) is a communication protocol for the secure exchange of bank files with any bank in France, Germany, Austria, and Switzerland. The EBICS infrastructures in France are subject to exemption rules for SCA. Germany and other Member States generally assessed that EBICS procedure are sufficiently secure and should not be in scope of the RTS on SCA and, therefore, not subject to exemption rules or transaction risk analysis.

engineering from the fraudsters, such as phishing. The implementation of SCA is not sufficient to prevent fraud in such instances.

Figure 14: Fraud rate for remote card payments reported by issuers and acquirers, with and without SCA, H2 2020.



Source: EBA (2022) Discussion Paper on EBA's preliminary observations on selected payment fraud data under PSD2, as reported by the industry

The latest Cybercrime report from LexisNexis, covering the period January to June 2021, shows that their Digital Identity Network has recorded a 623% growth in 3DS transaction volumes year on year and, encouragingly, has seen the eCommerce payments attack rate decline by 36% in the last 12 months. This is further evidence of the positive signs that are visible following the implementation of 3DS and SCA compliance programmes[198].

However, this data should be interpreted with caution as correlation does not imply causality. There are also other factors at play such as continued investment and use of innovative fraud prevention technologies by the industry. Indeed, a major international payment network reports that the SCA requirements together with technological developments have led to a reduction in eCommerce fraud rates of between 20%-30% since 2020. A BigTech, on the other hand, reported that even before SCA was enforced, they had been successful in reducing card fraud rate to below 0.06% and had recently reduced it even further (< 0.01%) through significant investments in combatting online payment fraud.

Stakeholders provided mixed feedback on the role of SCA in improving consumer protection. There are three broad categories of opinions: (i) those who agree; (ii) those who disagree and (iii) those whole believe that SCA his has brought higher security, but without creating the right environment for innovation. In the survey carried out within the framework of this study, respondents were asked to rate (on a scale of 1 to 5[199]) the extent to which PSD2 contributed to ensuring a high level of payment services users´ protection. 58% of the respondents stated that the PSD2 had contributed to ensuring a high level of PSU protection (rating of 4 or 5). In fact, only a minority (6 out of 62) seemed to believe that PSD2 had either not contributed to PSU protection or only to a small extent. Those who view that there are low levels of PSU protection argued that:

- The overall number of frauds and social engineering in digital payments has dramatically increased and is still increasing.
- Based on the fact PSD2 only covers payments accounts, ASPSP decided to restrict API to those accounts. As a consequence, all actors continue using historical technical

[198] LexisNexis (2021) Redefining trust and risk adapting to a post-pandemic world. The LexisNexis® Risk Solutions Cybercrime Report January to June 2021
[199] 1 for not at all to 5 for fully.

solutions to access other accounts (such as savings accounts). As a consequence, PSD2 application with API deployment have not had any positive impact on security as technical solutions to access accounts that are outside the scope of PSD2 have not evolved in the same direction.

- The protection with regards to data sharing (AIS) is much better compared to before (exporting CAMT/MT940 files and sending these), however, within the commercial APIs provided by banks, it is still possible for unlicensed parties to connect to banks creating a hole in the protection layer that PSD2 provides.

Some interviewees argued that while accounts might be more secure, consumers are incurring higher losses and are thus worse off. For instance, a major reported a significant increase (approximately 30%) in losses per fraud event. Several interviewees highlighted shifts in fraudster behaviour towards more sophisticated methods, either enabling them to overcome SCA (e.g., social engineering to obtain payment credentials, deploying OTP bots, etc.) or persuading a genuine customer to make a payment (i.e. payer manipulation).

SCA has led to increased complexity and friction in the payment process. Several industry representatives mentioned that SCA has introduced additional friction to PSU's everyday interactions. The initiation of payment transactions has become more cumbersome for customers. For instance, when a customer pays online using a PISP, the customer must use the PISP's app to initiate a purchase, then use another banking app from the ASPSP to complete the authentication, since the since responsibility for the authentication lies with the payment account provider (Plaitakis & Staschen, 2020). This increasing friction in the payment process, is reportedly causing a decrease in conversions in some countries although overall feedback on drop-off and abandonment rates is rather mixed. While some interviewees highlighted this as a major issue and provided data to support to their statements (reporting on average a drop-off rate of 20%), many payment institutions also indicated that this was not (or at least no longer) an issue. In countries where two-factor authentication practices were already in place (e.g., Sweden and the Netherlands) such a drop was not noticeable. In countries where it was not taking place previously the share of payments declined (or abandoned) rose, such as in France, Germany and Spain. According to one stakeholder interviewed: "SCA requires a level of friction that is quite hard to reconcile with smooth services such as wallet solutions and account-to account-payments (e.g., Apple Pay). This friction sometime leads towards user adoption of less/non-regulated payment as they are easier to use."

Consumer research undertaken in Germany by ECC Köln found that this friction is impacting on consumer payment behaviours. In response to a survey, 69% of the respondents indicated that they consolidated their checkout transactions with one payment provider/option, to streamline and facilitate the experience. And 35% of respondents indicated that they actively avoid certain payment options, where possible, precisely because of the SCA experience. Moreover, the same research indicates that SCA has also increased abandonment rates and complexity for consumers and had a negative impact on sales of merchants as well as banks and card issuers. Customers are asked for a second factor, which they may not always have with them, and this can lead to abandonment.

Previous studies underline increased frictions in the card payment experience resulting in abandoned sales, as the most important issue for merchants, who have no control under PSD2 rules as to whether SCA should be applied. (EPA, 2020; Plaitakis & Staschen, 2020). For June 2021, Patel et al. (2021) estimated the average failure rate of card payments at 25%, with the key reason being failed performance of 3D-Secure (3DS2). Countries where the estimated failure rates are above the EU average are Belgium, Germany and Italy at 38%, 33% and 29%, respectively. Previously, merchants had a certain level of discretion as to whether they would require further authentication from customers before accepting their payment. Although there are seven exemptions listed in the legislation, it is up to the customer's card issuer to decide whether an exemption can and should be applied. Since the payer's bank accepts the liability under SCA for authenticated orders that are fraudulent, they

have the control over the procedure and are able to delegate the authentication procedure to merchants. This puts the merchant in the hands of the bank, which could refuse the payment request, making the merchant unable to conclude these transactions.

Relayed to above, there is some evidence to suggest that SCA requirement has led to increased drop-off rates for certain financial products. For example, a company which helps customers build up a credit rating when they want to get onto the property ladder is experiencing a significant drop-off rate due to the 90-day SCA requirement. The company relies on continuous access to their customers account information so that they can build up their credit rating. They have high rates of sign up because it is an easy way for customers to build their credit ratings. But as soon as the 90 days limit is reached, their customers must go through their various bank accounts to authenticate each one individually and with different SCA approaches. This has significantly increased customer drop-off rates. An example was also provided of a very specific product in Portugal (one-time card for online transactions). Initially SCA was conducted when the card was generated. The national bank, however, deemed the card to be non-compliant because there was no linkage with the merchants at the time the card was generated. The card company thus had to introduce SCA at transaction level which resulted in a 15-20% dropout rate. Reduced use of potentially beneficial financial products eventually reduces consumer welfare. On the other hand, it could be argued that the fact that the SCA might "discourage" certain impulsive purchases to the benefit of consumers.

Consumers are also facing reduced choice of financial some products. The blanket prohibition on hybrid cards[200] was cited as an example. In February 2022, the EBA published guidelines on the limited network exclusion under PSD2. Under this Guideline, a single card cannot accommodate simultaneously open-loop (regulated) and closed-loop (unregulated) payment instruments, impacting products like meal vouchers, retailer cards or petrol/T&E cards. This provision is motivated by consumer protection principles: the EBA considers that such products are confusing for cardholders who do not realise that they do not have the same level of protection with unregulated payment instruments than with regulated ones. A major issuer suggested that instead of blanket prohibition, awareness among cardholders should be raised. There are many innovative hybrid card products already in the market, which provide real consumer value, and regulation should not prohibit such innovative products, but rather create a framework where these products can exist and continue to provide value to consumers and merchants alike, while at the same time being safe and secure. The purpose of PSD2 is to foster innovation in payments while ensuring safe and secure transactions and forbidding hybrid cards clearly impairs this balance between innovation and security at the expense of cardholders who benefit from the convenience and ease-of-use of such products. Hybrid cards have been allegedly widely adopted by consumers who would now need to be explained why these products are suddenly being removed from the market without at least a grandfathering regime being put in place. This measure also impacts European market players who have been using hybrid cards in different industries, e.g. meal vouchers and multi-benefits cards (e.g. Edenred, Up, Swile); retailer cards (e.g. Carrefour); petrol cards (e.g.Total).

Stakeholders claim that different groups of consumers are being impacted unevenly, but there is no hard evidence to verify these claims. Most forms of SCA combine passwords (knowledge) with some sort of form of device-based factor as possession (e.g., OTP, app-based notifications). Interviewees argued that this limits accessibly for less digitally savvy consumers (as consumers need to have the ability to navigate all the different methods of authentication) or those living in rural areas where digital connectivity could be poor. Several stakeholders argued that SCA is more suitable for younger consumers and those living in urban areas. There are also cost implications for consumers of acquiring a smartphone and data plan. Some of the most effective solutions, like biometric authentication factor, are effectively implemented only on modern mobile devices which results in uneven access to quality services for end customers and creates risks of digital exclusion.

[200] these provide an open-loop (regulated) and a closed-loop (unregulated) functionality at the same time

From the consumer perspective, literature underlines two main issues (1) accessing payment accounts and (2) the complexities faced by some consumers (such as the elderly) when adapting to new procedures (EBA, 2021a). Increasing digitalisation of payment services, coupled with lack of digital financial education of customers might lead to financial exclusion of vulnerable groups. When a customer pays online using a PISP for an online purchase, the customer and the merchant are connected through the establishment of an electronic link by the TPP. (Plaitakis & Staschen, 2020). Similar concerns have been raised by some AISPs, since PSD2 requires SCA every 90 days, which can create frictions during the procedure and increase the likelihood of customers dropping off from the service (EBF, 2021).

Moreover, from the perspective of some on the industry, aside from providing a sub-optimal user experience, SCA has had a negative impact on innovation as it is regarded as technologically prescriptive. Several industry players highlighted that PSD SCA requirements are prescriptive in defining the technological solution required to identify and reduce fraud. They explained that the rules prescribe active authentication techniques, with customer intervention, which limits choice for customers who might prefer to use frictionless solutions (such as Apple Pay and Google Pay). One BigTech argued that the requirement for the two factors to come from different categories is unnecessary; secure authentication in its view can also be conducted using two factors coming from the same category. Many claimed that a prescriptive approach to SCA is preventing the industry from applying more secure and friction less authentication alternatives based on behavioural biometrics[201], artificial intelligence and machine learning. It was pointed out that technology and innovation have a part to play in understanding the customer better and detecting fraud: machine learning, biometrics, historical snapshots to spot patterns and proxy detection are all tools to help determine whether a payment is fraudulent.

In this context, several industry stakeholders were highly critical of the EBA definition of biometrics (biometric solutions that incorporate a physical element such as fingerprints or facial recognition) In general, the term 'biometric' is understood to include both the physical and behavioural by the industry. EBA's opinion was seen to be an unnecessary narrowing of the types of biometric solution that could be deployed. It was argued that the introduction of behavioural biometrics would lead to more secure authentication mechanisms, more safe and with less friction for the consumer. One leading payments network provider was strongly in favour of a combination of behavioural biometrics and OTP and provided the following reasons to explain why it is stronger than SCA solutions based on the knowledge and possession factor: (i) accuracy – this combination captures new types of fraud which would be hard to capture otherwise, for instance in relation to risks of social engineering; (ii) security – It is considerably more secure as it is almost impossible to copy or replicate the data, similar to traditional biometrics (e.g., facial recognition, or fingerprint/iris scanning); (iii) inclusiveness – It is more inclusive and accessible especially as it does not require that devices be equipped with biometric sensors; (iv) better payment experience – Ultimately, it helps reduce transaction failure/abandonment rates (and consequently reduces harm to consumers and merchants).

Some stakeholders warned that a prescriptive approach to implementing SCA in Level 1 text gives rise to greater systemic payment ecosystem security risks. Several stakeholders warned that standardisation or homogeneity of SCA solutions is inherently dangerous as it increases the risk of fraud (the same fraud scheme can be easily duplicated).

Overall, there is a strong preference among stakeholders for outcomes and risk-based approaches to SCA. Stakeholders argued that regulation should set out principles and outcomes rather than prescribe specific secure technologies. This would future proof

[201] Behavioural biometrics, by contrast, looks at a range of behaviours such as typing patterns, speed of data entry, ways of holding a device or moving a mouse, against a stored user's profile to confirm the authenticity of the customer. With all data points taken together, a customer's digital footprint is built which is very difficult for fraudsters to replicate. Behavioural analytics solutions, such as 3DS profiling, are allegedly [please be more cautious in your qualifications] vastly superior in terms of fraud prevention compared to static knowledge factors. It creates a unique and dynamic profile for every cardholder, so there is a very low probability of an unauthorised party being authenticated as the payer

regulation against changing context, technologies, fraud practices, etc. Having an outcome-based approach to fraud prevention and widening the use of data for more effective risk-based decisioning would allow PSPs to deliver better on PSD2 fraud prevention objectives. A few stakeholders made the specific suggestion of "adaptive authentication" approaches that distinguishes the strength of authentication required for each type of activity based on its risk. Such a framework can include a risk score(s) as part of the authentication mechanism to reduce friction, e.g., instead of requiring two factors, it can require one factor and a low risk score (logically implying that the PSP has a level of assurance in the identity of the client and the real-time risk assessment shows no / low quantifiable risk); if the risk score is high, that would trigger the second factor (=SCA). Moreover, it was explained that all pillars of risk management business models, financials, intent, customer identity etc. are needed for effective management of fraud risks – simply focusing on customer identity is not enough to ensure a robust framework. Several industry players suggested the use of risk-based approaches using state-of-the-art ML/AI-based capabilities to better monitor transactions, understand consumer behaviour and detect fraudulent behaviour.

One of the PSPs interviewed explained that the objective of increased security is best achieved through adaptive methodologies and recommended that authentication be based on a 'layered defence' model, thus ensuring a risk-based and outcomes-based approach to SCA. PSD2 is based on the assumption that every transaction is high risk and needs SCA, except in very specific cases (exemptions). Some PSPs interviewed have argued that SCA should be triggered only when transactions triggers certain risks. In other cases, 'simple authentication', backed up by robust and continuous risk management should be sufficient to ensure both security and consumer protection, as well as foster innovation and economic growth.

Though not specific to PSD2, some stakeholders also expressed concerned about the amount of data that is being collected by payment networks for 3DS solutions. It was repeatedly emphasised by several interviewees that 3DS2 requires more data fields as compared to 3DS1. They explained that with 3DS 2 there are 150-200 additional data fields and merchants must submit a large amount of data. According to the interviewees, this mass collection and storage of data by payment networks is being done in a way that is not transparent to the customer and serves no benefit in terms of reducing fraud.

Conclusions and considerations

Fraud levels have declined following the introduction of SCA requirements, but how much of this decline is attributable to SCA is not known at the moment. Nonetheless, it is fair to say that SCA has been a catalyst for the industry (issuers, acquirers, merchants) to strengthen their fraud defences through greater use of real time systems and stronger fraud rules.

The evidence suggests that the SCA rules lack clarity and the RTS are overly prescriptive on certain aspects. This has limited innovation and prevented PSPs from developing more advanced and effective solutions to prevent fraud.

Stakeholders have made several suggestions:

- Provide greater clarity on scope (e.g., MOTO transactions) and exemptions. In this context, one stakeholder suggested that several rules that are in level two, should be in level one. Moreover, the RTS should be sufficiently clear and avoid excessive reliance on Q&A for answers.
- Having an outcome-based approach to fraud prevention and widening the use of data for more effective risk-based decisioning.
- PSD3 should allow for behavioural biometrics and data inherence to be considered authentication. PSD3 should not consider wallet and merchant authentication as outsourcing.
- PSD3 should consider expanding the manner in which the SCA and transaction risk analysis audit requirements may be satisfied. It may also be beneficial to consider

whether there is scope for meeting the audit/testing requirements through other means than traditional accounting/statutory audit provisions.

- SCA exemptions should include EUR 0 authorisation/verifications process. In line with Article 97, credit institutions should not require strong customer authorisations (SCA) for account verifications, i.e. EUR 0 authorisations. Credit institutions SCA requirements for EUR 0 authorisations add considerable friction to the customer experience/on-boarding and do not create any extra level of security as SCA is applied to any future payment in any case.
- With regards to contactless transactions, it is suggested to increase the current SCA per transaction thresholds for contactless from EUR 50 to EUR 100, and to increase the cumulative threshold accordingly. We would welcome a dialogue with payment stakeholders and regulators for where this cumulative level could ultimately be set, but we suggest at least EUR 250 or five consecutive taps.

To promote contactless innovation, and facilitate socially beneficial consumer behaviour, the industry recommends extending the current SCA exemption for unmanned parking terminals to include unmanned electric vehicle charging stations and charity donation stations. It is disproportionate in their view to request SCA for transactions of very low amounts at vending machines and donation terminals, and they should benefit from the same exemption as the unattended terminals for transport and parking. Fraud data do not suggest higher fraud rates for vending machines or donation terminals compared to transport and parking machines, while the average transaction value is lower both at vending machines and donation terminals. As the nature and environment of electric (alternative) vehicle charging transactions is very similar (and in some cases identical) to those of transport and parking transactions, it would both make economic and social sense, and ensure legal consistency, for electric vehicle charging and alternative fuel filling transactions at unattended terminals to benefit from the same exemption.

5.2.9. Rights and obligations (e.g., regarding charges, liability and recovery of damages)

Banking representatives claim that the burden of fraud disproportionately falls on them, but this is not corroborated by facts. According to data compiled by EBA, PSUs bear most of the losses due to fraud relating to credit transfers and cash withdrawals, even though Article 73 of the PSD2 provides that liability for unauthorised transactions should lie primarily with the PSPs (unless the user has acted fraudulently). According to EBA data, PSUs bore 68% of the losses due to fraudulent credit transfers and 60% of the losses due to fraudulent cash withdrawals in H2 2020. According to EBA, this pattern could partially be explained by the fact that under Article 74 of the PSD2, the PSU bears the losses relating to any unauthorised payment transactions due to the PSU acting fraudulently or failing to fulfil its obligations as set out in Article 69 of the PSD2 with intent or gross negligence. In particular, the events covered by the notion of gross negligence might be differently understood and applied by the market stakeholders[202]. Moreover, stakeholders report that consumers often lack awareness of their rights and obligations. This lack of awareness could result in them unfairly bearing the burden of fraud.

Banking representatives also called for the introduction of mandatory waiver of liability provisions for corporate payments (instead of having it as optional). According to them, there are differences across Member States as regards the types of businesses that are subject to the waiver for corporate payments. In this respect, it was clarified that the waiver is necessary for large corporates rather than SMEs.

More generally, representatives of PIs highlighted several inconsistencies within PSD2 and made numerous suggestions for improvement. These are summarised below.

[202] *EBA (2022) Discussion Paper on EBA's preliminary observations on selected payment fraud data under PSD2, as reported by the industry*

Right to a refund for direct debits not being consistent across all types of payment transactions. It was suggested that this rule be extended to all types of MITs.

Allocation of liability without requiring SCA. It was pointed out that while Article 74(2) explicitly refers to the payee, Article 98 does not grant exemptions from SCA to the payee.

Maximum limits for the amount to be blocked on the payer´s account when the amount of the payment transaction is not known in advance (this rule is not consistent as it refers to cards only).

Calculation of fraud rates. European jurisdictions have taken divergent stances on the interpretation of the calculation methodology (e.g., Germany vs Ireland). EBA has provided comment on the calculation methodology through both the publication of the 13 June 2018 Opinion and the EBA Q&A 2019_4702. (So-called 'net' calculation vs 'gross' calculation). Nonetheless, the divergence in regulatory interpretations on the calculation methodology across jurisdictions was seen to be unhelpful, and it was suggested that one clear method of calculation be used across EU jurisdictions.

The liability regime under Art. 73 relating to unauthorised payments. According to Article 73(1) of PSD2, Member States shall, without prejudice to Article 71, ensure that in the case of an unauthorised payment transaction, the amount of the unauthorised payment transaction is refunded to the payer by the payer's payment service provider without undue delay, and in any case no later than the end of the next business day after the recording of the transaction or after having received a notification to this effect, except where the payer's payment service provider has reasonable grounds to suspect fraud and notifies the relevant national authority of the grounds in writing. One day for reimbursement is considered too short for a proper investigation of liability, reimbursement and blocking of funds. Stakeholders argued that having to return funds without sufficient time to verify a potentially unauthorised transaction involves a risk to the security of the funds entrusted. It was suggested that reimbursement period be extended to at least two business days. It was also questioned whether the requirement to refund an authorised payment immediately is always in line with a PSP's requirement to duly examine the incident: it was explained that assessing the information presented by the PSU and their technical circumstances in a proper manner requires several business days. This is particular true in ambiguous cases, where the bank would have to bring forward allegations of fraud against their customer in order to gain time for a sufficient examination and safeguarding their rights. Also, when a TPP is involved in the payment, the investigation and resolution of such complaints is more complex and often requires more time. Furthermore, it was suggested that a harmonised resolution framework for the handling of customer complaints related to unauthorised payments between ASPSPs and PISPs, including minimum response deadlines and standard communication channels, might support the efficient solution of cases and reduce risks for all parties involved.

Another stakeholder suggested that the timeframe for reimbursement according to Art. 73 (1) should be differentiated:

- if the payment was initiated without a PISP being involved, it could remain as it is;
- if a PISP was involved, extend it by 24 hours; and
- if the ASPSP has reasonable grounds for suspecting fraudulent behaviour by the PSU submitting the complaint, it should be allowed to investigate longer before reporting the PSU to the NCA, but block the funds.

Another stakeholder explained that the deadline in the Directive only allows for verification of system records, not explicit knowledge of fraud. They proposed to extend the deadline for refunding an unauthorised payment transaction or make the start of the period for refunding the amount of an unauthorised payment transaction conditional on the provider confirming the accuracy of the customer's claim of unauthorised transaction or obtaining such information from another source.

In addition, the current wording of the above provision is often interpreted as exempting customers from liability for transactions resulting from their careless and reckless use of payment services. Several stakeholders suggested that the EU legislator should require an appropriate standard of conduct from consumers. One stakeholder suggested that consumer benchmarks should refer to the average, but prudent, consumer who makes informed use of payment services. The directive should include provisions on the standard of the average, prudent consumer, with examples of behaviour considered grossly negligent.

Another key point is to achieve a more balanced allocation of liability between ASPSPs and TPPs, especially regarding unauthorised payment transactions. Where the payment transaction is initiated through a PISP, the ASPSP shall refund immediately, and in any event no later than by the end of the following business day the amount of the unauthorised payment transaction and, where applicable, restore the debited payment account to the state in which the unauthorised payment transaction would not have taken place. If the PISP is liable for the unauthorised payment transaction, it shall immediately compensate the ASPSP at its request for the losses incurred or sums paid as a result of the refund to the payer, including the amount of the unauthorised payment transaction. In accordance with Article 72(1), the burden shall be on the PISP to prove that, within its sphere of competence, the payment transaction was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency linked to the payment service of which it is in charge. Given the fact that the PISP relies on the authentication procedures provided by the ASPSP to the PSU the burden of prove will de facto almost always lie on the ASPSP. Moreover, the ASPSP must immediately compensate the PSU and is entirely dependent on the solvability and willingness of the PISP for its compensation. In general, the liabilities and risks in the PSD2 are not fairly balanced between ASPSP and PISP/AISP. It was suggested that ASPSPs should be able to limit access to certain TPPs when fraud rates are significantly higher, especially if they show no intention of taking any measure to cooperate and take measures to avoid and prevent fraud to happen. PSD2 should modify the obligation of the ASPSP to immediately refund the payer when TPPs are involved and include measures or instruct EBA to work on a disputes protocol to assign liabilities and to allow ASPSPs to actually claim the sums to be paid to the payer as a refund. Regardless of the underlying payment instrument and a possible involvement of a PISP, it is questionable whether the requirement to refund an authorised payment immediately is always in line with a PSP's requirement to duly examine the incident.

Finally, it was mentioned that rights and obligations between PSU and PSP regarding fraudulent payments must be limited to non-authorised payment transactions. Extending these to damages resulting from a fraudulent underlying business transaction or social engineering would not be appropriate since it does not relate to the PSP's sphere of influence and the security of its systems.

Art. 73, reporting requirements that should be reviewed to see if it is an effective process and how this information will be used. When an ASPSP decides that there is a need for an additional investigation, in each instance they are required to inform the supervisor about this (within 24 hours). This requirement is considered a heavy administrative burden. They suggested the possibility to bundle the information or to document about such type of event without the need to automatically send in a response every time.

The interaction between Art. 80(2) and 80(4); and if 80(4) overrides 80(2). According to several banks there is lack of clarity when looking at EBA opinion 2018.04. The answer from EBA says that the payment can be recalled if it has been concluded between the ASPSP and the payee, the PISP does not have to be involved. This could be understood as Article 80(4) would be superior to 80(2). The reasoning is that this can lead to Art. 80(2) becoming void and would therefore no longer serve any purpose. It was suggested that the clarifications provided by the EBA Q&A should be implemented in the directive.

Removal of Art. 75. It was argued that it is not reasonable that a card issuer is liable for what information is shared by the merchant at the moment of transaction.

Some terms used in PSD2 with regards to rights and obligations are considered to be vaguely defined, e.g., "misappropriation", "payment instrument". It is not entirely clear what is meant by these definitions especially when it comes to new ways and forms of providing payment services online and deciding whether and how particular circumstances related to usage of payments services and payment instruments fall into one of these categories.

There are different interpretations of what is meant by "fraud" as per Article 73 of PSD2. The difference between the de facto assumption of article 72 of PSD2 ("when a user of payment services denies having authorised a payment operation") and that of article 73 ("in the event that a payment operation is executed unauthorised"). Both entities and users usually confuse both assumptions. This could be done within the framework of the definitions.

The definition of fraudulent action and gross negligence in point 2 of article 72 and in the second and third paragraphs of point 1 and point 3 of article 74 of PSD2. At present, it is not clear how an entity can prove such fraudulent or grossly negligent action. They frequently accredit it through proof of the use of one or more security elements (PIN, OTP, push notification, etc.), but it is not clear if this is enough to consider that negligence or fraudulent action concurs.

Art. 74(2) is considered ambiguous by some stakeholders. Under art. 74(2) when establishing the payer's liability, fraud is cited as the exclusive reason for the payer to be obliged to bear any losses up to the maximum of EUR 50. However, if the payer failed through gross negligence to detect any loss, theft or misappropriation (in circumstances where the payer's failure did not amount to fraud), then it could still be said that detection by the payment services provider was not possible. Also, the wording of art. 74(2) suggests that for liability to shift from the payer to the payment services provider, the relevant PSP's action or omission must have caused the loss. It is not clear what determines causation/causality for this purpose (e.g., whether the action or omission of the PSP/agent must be the sole cause, main cause or contributory). The only certainty in the way that art. 74(2) is currently drafted is that where a payer acted fraudulently then the payer must bear all the losses of the relevant unauthorised transactions. Apart from that, it is not sufficiently clear in what circumstances a PSP may exercise their discretion and require a payer to be liable for the maximum liability of EUR 50.

There is a confusion in what can be considered an unauthorised operation, which gives a false sense of security to the user who believes that any operation that he considers unauthorised will be returned regardless of the level of diligence that he has displayed in relation to the transaction. Custody of security elements. The user usually believes that the payment service provider is going to be responsible in any operation in which it is proven that fraud has occurred. It was suggested that, in order to promote greater effectiveness of the provisions set forth in Chapter IV of PSD2, regarding the rights and obligations in relation to the provision and use of payment services, it would be appropriate to clarify when the exception a) of point 1 of article 74 is applicable, that is, when "it was not possible for the payer to detect the loss, theft or misappropriation of a payment instrument", in which case, the payer may be obliged to bear, up to a maximum of EUR 50, losses arising from unauthorised payment transactions resulting from the use of a lost or stolen payment instrument or the misappropriation of a payment instrument.

There needs to be more accountability on the user side in the online world. Several stakeholders suggested that the maximum liability for a payer resulting from the use of a lost or stolen payment instrument or from the misappropriation of a payment instrument should be reassessed and potentially increased in order to reflect inflation and also to discourage careless or reckless behaviour on the part of the consumer. Furthermore, Member States should not have a possibility to derogate the maximum liability of customer as this creates differing treatment across the EU for different consumers.

It was suggested that the exception in article 74 (2) "fraudulent act by the payer" should be extended to include "intent" and "gross negligence". There should be a definition of gross negligence, with examples where consumers would be liable instead of the PSP (to keep a

healthy balance between consumer protection but also protecting PSPs, as well as providing a level playing field across EEA) such as: sharing payment credentials including OTP with third parties; allowing others to use one's device with their biometrics (e.g., fingerprints) enabled and stored in the device; payments where amount and merchant were displayed to consumer, e.g., during authentication, do not (fully) reflect the intended payment – this explicitly includes merchants whose name resembles known entities (e.g., tax office, police) which means that if in doubt consumers should check with the impersonated entity whether they actually requested the payment. Future regulation should recognise and define cases and instances of fraud where consumers should partially or entirely bear the responsibility.

There is some ambiguity in interpretation of rules regarding framework contracts and single payment transactions. According to representatives of TPPs, it should be clarified that some service providers can act without any contract requirements on the payer side. There are currently different views on whether this is possible, in particular for (merchant-facing) PISPs[203], which places them at a competitive disadvantage compared to card acquirers and card processors.

There are differences in interpretations by Member States on how changes to framework contract conditions should be implemented. The position taken by some Member States is that changes need to be expressly agreed by customers, whereas PSD2 does not require this. Representatives of TPPs emphasised that a change of framework contract conditions should require active acceptance of the PSU (implicit acceptance should not be allowed).

The surcharging ban has been highlighted as an issue by many of the stakeholders interviewed. The surcharge ban under PSD2 aims to protect consumers across Europe by prohibiting merchants from charging consumers additional fees for making payments with consumer debit and credit cards, both in shops and online. For example, merchants, including ticketing, travel and food delivery websites are no longer allowed to charge consumers additional fees for paying by debit or credit card, and they can only steer them to less expensive means of payment through rebates. However, some stakeholder interviews (e.g., EU associations) and press reports suggest that the surcharging ban has resulted in an increase in prices[204]. Some card issuers (e.g., Visa and MasterCard) have increased scheme fees to make up for the lost revenues or merchants have circumvented the ban on surcharges by incorporating the extra processing costs of accepting such cards in their retail prices. Either way, it is the consumer who pays in the end.

Generally, one could say that the surcharging ban helps to create a level playing field between payment instruments and create a much clearer picture for consumers in which they know the full price of the product or service they are purchasing upfront and are able to avoid hidden and unfair surcharges. On the other hand, from the point of merchants, it seems that the change on the surcharging ban mostly affects smaller merchants or those in industries that typically operate with low margins and that need to find an appropriate way how to offer payments with well-known payment instruments while absorbing the processing costs. Several stakeholders mentioned that the surcharging ban potentially contributed to the faster shift towards popularisation of certain payment methods e.g., digital payments.

Some PSPs that are in favour of the surcharging ban suggest fully extending it to non-card payments. In practice, surcharging is fully banned in most Member States, which has fostered the adoption of alternative payment providers in those markets. According to a large international PSP, merchants have seen the benefits of the surcharging ban via increased sales.

[203] Merchant-facing PISPs need consent from both the payer and the payee/merchant to initiate a payment between the two, but they are acting solely on behalf of the merchant and a contractual relationship is only needed there. On the payer side, it is sufficient to obtain (GDPR-type) consent without the need for a single payment contract.
[204] Guardian (2018) End of the great card payment rip-off? No, it's just a new one

5.2.10. Data access and data sharing

PSD2 was a major step towards laying the foundations for a future open finance ecosystem in the EU. PSD2 mandates regulated ASPSPs to provide licensed TPPs with access to their customers' accounts. By getting direct access to a customer's account, TPPs such as FinTechs and e-commerce businesses are able to build services on top of a bank's existing data and infrastructure, thus providing consumers with a range of new services for managing their finances. More widely, the opening up of access to large data pools through the extension of open finance principles, along with the innovative application of technologies such as machine learning, holds out the potential for faster, more convenient, more innovative as well as safer and more inclusive payments for European merchants and consumers. Stakeholders acknowledge that PSD2 has been a driving force for numerous initiatives and market-driven standardisation like the API Access Scheme Working Group, which are important elements for an open finance ecosystem.

While PSD2 has unlocked the potential for open finance in Europe, there are several issues constraining its overall effectiveness. PSD2 requires ASPSPs to set up open APIs or to provide access through the consumer online interface, but it does not specify a standard format across the EU to allow access to accounts (XS2A). Consequently, several issues have emerged following the implementation of PSD2. These issues can broadly be grouped into four categories: (i) data access; (ii) data sharing; (iii) consent and data protection; and (iv) API standards. These are explained in the sub-sections below.

Data access

TPPs report experiencing a multitude of issues, many of which act as obstacles for the provision of payment services.

Several TPPs reported that a number of ASPSPs have not fulfilled their obligation to implement the PSD2 rules on access to and use of payments account data. PSD2 and the RTS are drafted in a way that allows considerable room for interpretation, and consequently TPPs and ASPSPs disagree on what data is accessible via the ASPSP's dedicated interfaces and what are the requirements to access the PSU's data. It was reported that some ASPSPs have started "gatekeeping" the data TPPs can access.

A key problem seems to be lack of data parity between PSD2 API and ASPSP's other customer-facing interfaces. TPPs report that the support of authentication methods, data exchanges and ease of use of the PSD2 APIs have not been equivalent to the experience offered by the ASPSP's in their other customer-facing interfaces, despite the clarifications made by EBA as regards the obligations each ASPSP has in regards to the functionality of the PSD2 API.

On major problem relates to missing or inconsistent data. TPPs report that they cannot retrieve as much data from the PSD2 APIs as they would be able to retrieve via the direct access methods. Some TPPs explained that when they notice this issue, it is reported to the relevant ASPSP. Some ASPSPs comply with their requests and add the missing data. But there are also those who do not agree with TPPs' request as they have another interpretation of what data should be available in accordance with PSD2 and the RTS. Typical issues encountered by TPPs in this regards are as follows:

- Data, such as the name of the account holder and/or or the IBAN selected for the payment initiation, are missing. The ASPSP may also not report what fees are charged for the payment as well as whether the PSU's selected account has enough balance to cover the payment.
- The account balances are not calculated the same way in the PSD2 API as on the online banking portal. For example, the balance could be calculated without overdraft limits. In some cases, there are missing transaction categories (pending or cancelled transactions are not available on PSD2 API although this information is available in the online banking portal).

- Not as much transaction history is available in the PSD2 API as in the online banking portal. For example, AISPs could potentially only access 30 days of transactions history while 90 days is available in the online banking portal.

It was argued that basing the scope of the data to be shared on the principle of non-discrimination has turned out to be unsatisfactory with regards to legal certainty. In practice, there has been much controversy what constitutes "information from payment accounts and associated payment transactions", with answers only being provided through a drawn -out Q&A process. Some stakeholders called for providing in the PSD and/or EBA RTS a list of necessary data to be shared. Data points that are on this list should be available to TPPs as long as they are available in the customer interface. Certain data points might even be made obligatory, even if they are not available in the customer interface (as long as they are known by the ASPSP). Data points that are not on this list are not obligatory, even if they are provided in the customer interface. The list should be updated regularly, with an appropriate implementation time for new entries. The appropriate legal instrument should be a guideline, given that it is very time consuming to change an RTS.

Additionally, stakeholders pointed out that PSD2 is extremely restrictive around what a TSP or TPP can do with the data they see flowing through, or the data being used in the provision of the service. There are a few areas where this is restrictive and potentially not in the best interest of the PSU:

  - There is no exception for counter-fraud or AML purposes. TSPs are reliant on other legislation to carry out this activity. PSD2/PSD3 should be explicit in the appropriateness of this.

- **Another big issue relates to poor authentication procedures and their negative impact on TPPs' services, particularly where redirection is used.** Three key issues were reported by TPPs in this regard:
- TPPs generally argue that redirection makes customer journey unnecessarily complex, leading in turn to lower conversion rates for TPPs (i.e. high churn rates every time SCA is applied). Redirection indeed creates a level playing field issue between TPPs and ASPSPs as the former depend on the quality of the redirection procedure provided by the latter. Many ASPSPs support a redirect authentication approach, where the PSU does not perform the complete authentication process in the TPP's domain, but instead they are redirected to the ASPSP to enter their anonymised security credentials and perform the SCA before the PSU is returned to the TPP. Consumers can be discouraged to start using TPPs' services, especially consumers that are using TPPs' services for the first time. Even if an ASPSP offers a redirect authentication approach in their PSD2 API, where the PSU is redirected to the ASPSP to perform the authorisation procedure, the PSUs may be hesitant to enter their data. ASPSP's redirection pages for the PSD2 API could look very different from the pages that the ASPSPs present in their other customer-facing interfaces (e.g., online banking portal or mobile banking app) and the PSU may believe that someone is attempting to defraud them by impersonating their ASPSP. As an alternative solution to this issue, which is particularly crucial for the AIS, it was suggested that PSD3 could consider that AISPSPs can issue their own security credentials to allow the access to the accounts after an initial SCA carried out by the ASPSPs.
- TPPs reported that there are some ASPSPs that do not support all authentication methods in their PSD2 API, which are instead available to PSUs in other customer-facing interfaces, despite Articles 97 PSD2 and Article 31(2) RTS (which explicitly state that ASPSPs shall allow PISPs and AISPs to rely on the authentication procedure provided to the PSU). The EBA even clarified in 2018 that all methods of SCA provided to the PSU need to be supported in the PSD2 API when an AISP or PISP is used, and that PSD2 API implementation that did not do this would create obstacles to the provision of TPP's payment services – EBA-Op-2018-04 paragraph 50).

- Some ASPSPs require the PSU to perform multiple authentication/SCA steps in the PSD2 API than what would be required to the PSU in other customer-facing interfaces. This is despite the fact that EBA has deemed this practice as an obstacle to the provision of TPP's payment services in accordance with Article 32(3) RTS (EBA/OP/2020/10 paragraph 22 – 28).

TPPs also reported having experienced lack of support and a worst user experience for authentication flows on mobile devices, despite an increasing number of consumers using their mobile devices for AIS and PIS services. For example:

- The redirection pages of the ASPSP are not adapted for mobile devices' screen and size. For example, the PSU may have to scroll or click several times to see all the information presented by the ASPSP relating to the authentication.
- The redirection pages do not have the same look and feel as the PSU expected, or are considerably different from what is presented in ASPSP's other customer-facing channels, which could create suspicion and discourage customers from using the AISPs/PISPs' services.
- The ASPSP redirects the PSU to a web-based browser instead of redirecting them to their already installed mobile banking application. Some ASPSP do not have automatic redirects, meaning that the PSU is required to manually switch between apps to go through the authentication flow. PSUs may expect to be automatically redirected, and think that something has gone wrong and doesn't manually open the mobile application.

The EBA has clarified that ASPSPs must ensure that AISPs/PISPs can rely upon the authentication procedure(s) provided by the ASPSP to the PSUs. More specifically, ASPSP shall enable the PSU to authenticate themselves with the ASPSP's provided mobile banking app for AISPs/PISPs' services if provided in other channels (see EBA/OP/2020/10 paragraphs 11 – 16). Despite that the EBA clarified the above in 2020, PSUs are reportedly still experiencing these difficulties in 2022.

APIs lack support for all payment accounts. Industry stakeholders pointed out that more clarification is needed that the PSD2 applies to all types of payment accounts, including business and corporate accounts. Reportedly some ASPSPs have either not implemented business/corporate accounts in their PSD2 APIs or business/corporate accounts are included, but business customers are required to opt-in in order to use PSD2 API

ASPSPs' API documentation is not sufficient. In many cases, TPPs have also encountered that what the ASPSP has described in its documentation was not correct for the implementation of the PSD2 API. They were required to contact the ASPSP for further clarification to fully implement their API which involved additional time and resource investment from TPPs. This is despite the fact that Article 30(3) RTS states that ASPSP shall ensure that the technical specifications of their interface are documented and specify the set of routines, protocols and tools needed to allow TPPs to interoperate with the ASPSP's system. A requirement stemming from RTS is that the documentation available must be correct and sufficient so that TPPs can connect securely.

There are no penalties for non-compliance by ASPSPs. An NCA should ensure that ASPSPs remove the obstacles to ensure compliance with PSD2 and the RTS. However, apart from complaining to the NCA, there are no other mechanisms for ensuring that ASPSPs comply with the regulations. ASPSPs can potentially be non-compliant for several years without consequences that would penalise the ASPSP for their breach of regulatory obligations towards both TPPs and PSUs. One stakeholder explained that NCAs have not been able to sufficiently enforce ASPSP compliance with PSD2, due to lack of resources and/or the technical understanding to get to the bottom of the problems with the APIs.

Finally, it was pointed out that there is no recognition of the need to conduct reporting on both PSU and/or ASPSP activity. For example, an ASPSP may wish to understand their activity in the context of the wider market and understand where their performance (e.g., API

response time) does not meet market benchmarks. There should be provision for TSPs/TPPs to use anonymised and aggregated data to provide reporting services back to both PSUs and ASPSPs.

Remuneration for access to data on payment accounts

Banks are critical of the principle that they must provide TPPs with free of charge access to their customers' payments account data. This, they argue, amounts to an unfair and regulatory-driven competitive disadvantage. According to many interviewees, a key prerequisite for an open data framework to be successful is the possibility for banks to monetise the data they hold. Banks incur costs in maintaining accounts, processing payments and investing in infrastructure to share this data with TPPs. According to these interviewees, there should be no prohibitions for banks in monetising these data.

Some interviewees went as far as stating that this principle of the PSD2 (free of charge access to data by some market participants, held by other market participants) is hampering investments in innovation and competition. As ASPSPs must provide free-of-cost access to the data they hold, there is no incentive for them to invest in innovation in this area. Moreover, they claim that there is an opportunity cost to the investments they have made in providing TPPs access to data. Moreover, one party is now expected to provide an infrastructure at no cost to an entity that in turn can capitalise on this infrastructure, thus creating regulatory-driven competitive disadvantage for banks.

Data sharing

It was also suggested by banks that clarifications be provided in the Directive regarding the delineation between services that ASPSPs must make available to TPPs via their PSD2 APIs free of charge on the one hand, and on the other hand "premium" services or added-value functionalities that go beyond the scope of the PSD2 requirements. It was pointed out that compelling ASPSPs to provide innovative 'premium' solutions (either enhanced functionalities or features or data beyond what is currently required under PSD2) to TPPs free of charge may hamper market innovation and the willingness of ASPSPs to develop and invest in such innovations in the future.

Some stakeholders also questioned the four-times-a-day limit to access data for APIs (RTS on SCA &CSC, art. 36), arguing that when there is a dedicated interface, and access is not degrading their performance vis-à-vis the customer, it does not make sense to have a limit.

Consent management

A transparent consent and permission framework is a prerequisite for open banking/ open finance. A foundational element of open banking is that it empowers consumers as they make their own choices to bring their data together from multiple sources, and then use that information to inform their financial behaviours and decisions. Trust in the security of access to financial data is therefore, a key factor for a successful 'open banking' or 'open finance' framework. Rules need to be defined to achieve a high level of security, balanced with convenience and transparency. The customer needs to understand when and why to provide consent/permission – if this depends on too many variables along the payment value chain between payer and payee, this can impede transparency. According to one interviewee: "In the current definitions in PSD2 and the technical standards, for example, many rules and exemptions are defined with good intentions from a security perspective but are overly complex from a user perspective."

Stakeholders highlighted several weaknesses with PSD2 as far as consent and permission management are concerned. These are summarised below:

- There is no option for consumers to centrally manage the permissions that they have given (i.e. a mechanism for obtaining an overview of the consents given and an option to revoke consent from there.)

- The way that the client can revoke consent is not well developed. A consumer cannot revoke access from the TPP through the TPP itself, but only through the ASPSP. Many times the client is not aware that they have provided consent to a TPP, so they just go to the ASPSP, with which they are used to interacting, to ask for revocation of the consent, but as the consent has been given to the TPP, the ASPSP cannot revoke it.
- The 90-day consent period **(resulting from the Level 2 legislative process)** is perceived to be detrimental to the consumer's experience. **It is said to be cumbersome and has dissuaded consumers from using AIS services on an ongoing basis.** Currently, consumers using open banking services that give TPPs, such as apps or peer-to-peer (P2P) lending platforms, access to their main bank account must reconfirm permission every 90 days. While the industry appreciates EBA's recent proposed amendments to extend the renewal timeline to 180 days, they feel that it does not fully address the impact on the customer journey. Several alternative solutions were proposed: (i) descoping AIS from the PSD2 and addressing such data exchanges under the upcoming open finance framework, where a consent-driven model could be implemented (see also discussion on scope of PSD2); (ii) to amend article 97 of the PSD2 to make it clear that once a PSU authorises an AIS to access their payment accounts (through a mandate for instance), then that permission is valid on an ongoing basis until the PSU revokes access. This would allow AIS services to drive more seamless experiences in the EU, while enabling customers to control their data. Allowing the consumer to set the consent period, or even just reminding them of the possibility to retract consent instead of having to give it every 90 days would make for a smoother consumer experience.
- There are issues with consent management in certain ASPSP's PSD2 API which mean that the PSUs may not be correctly informed of what their consent means. There are also problems with the specifics of the consent, especially if an ASPSP's PSD2 API does not allow for customisation of the consent concerning its duration – explained in the box below.

APIs do not allow customisation of consent duration and scope

This is particularly an issue in relation to Article 10 RTS. Article 10 RTS provides an exemption from the SCA when a PSU or AISP accesses account information for a period of at most 90 days after the first initial access using SCA. Although Article 10 RTS allows AISPs to access the account information for 90 days without any need for additional SCAs, an AISPs may wish to access the account data for a shorter period of time or even for just one single point in time. However, some ASPSPs' APIs do not enable the AISP to request access to account data for less than 90 days. In other cases, TPPs have experienced that ASPSPs the AISP to request less than 90 days access, but the ASPSP, instead, informs the PSU during the authentication procedure that the AISP is requesting access to the user's account data for 90 days anyway. Similarly, the ASPSP may also inform the PSU which data types the AISP can access (e.g., list of accounts, account details, balance on an account and lastly transaction on an account). In this context, the ASPSP may inform the PSU that the AISP can access all the data types even if the AISP may only have requested access to one of them. This issue is often caused by the fact that the text displayed to the PSU on the ASPSP's AIS redirection page is created only for the case where the AISP is requesting access to account information for a maximum amount of time and for the maximum amount of data. As a consequence, the information displayed by the ASPSP to the PSU is not only incorrect but could discourage customers from using the AISP's service. Furthermore, the scope of the consent cannot always be immediately recognised in the ASPSP's domain during a redirect. It might be the case that a PSU first has to go through multiple login steps before learning which permissions they are being asked to grant. This might discourage PSUs from proceeding because they might fear they could agree to something "accidentally" by logging in without knowing what it is they are agreeing to.

- Some stakeholders reported that some ASPSPs provide text that asks consumers to consent to more privileges for the TPP than are needed for the provision of the service. This has implications for the trust between the consumer and the TPP. It was suggested that consent texts should be regulated to be more relevant to the authorisation needed by the regulated TPP and not as generic text. In this context it should be noted that the EBA has clarified to some extent with regards to consent related text in conjunction with SCA (See issue ID XXVII from the EBA API WG).
- Consumers do not normally understand the finer details of what they are giving consent to. Consent text is written in such a way that it generates distrust as it is not easy to understand, and this also means that many people do not read the text.

Interviews offered several different solutions as follows:

- A consumer should be able to specify the exact period for which they consent to sharing their data; retract a particular consent at any time; and obtain an overview of all the parties that they have given consent to, within the digital environment of their AISPs.
- Level 1 text must make it fully clear that it is the TPP that handles the consent of the user and that this is done without involvement of the ASPSP. Moreover, PSUs should have the possibility to revoke any provided consent even via the ASPSPs. The PSU as the data owner should have the full control regarding any provided consent. It should be clarified in Level 1 text that PSUs can instruct their ASPSP to revoke consents given to a specific TPP. The ASPSP has the consolidated information on any consents. If it is the PSU instructing the ASPSP to revoke the consent this cannot be interpreted as an obstacle to TPPs. But what should not be allowed is any type of recommendation given by the APSPS to their customers to revoke any consent as this would be a clear obstacle.
- Global consent would be preferred before bank-offered and detailed consent[205]. This is due to issues experienced with opt-in consent to specific scopes (accounts, account details, balances, transactions) since the PSU may choose not to include a scope that is vital for TPPs to be able to provide the payment service.
- One consumer protection agency suggested that the EDPB Guidelines should be turned into law to become legally binding for providers. They reiterated that payments account data is highly sensitive. This is particularly the case for (but not limited to) Article 9 data. Consequently, consumers should know what to expect when using an AISP. Legislation should foresee either a positive list or a negative list of use cases. For example, a negative list could contain credit scoring. This would allow consumers to use AISPs (e.g., a multi-banking app) with confidence and without risking potentially disadvantageous effects on their economic wellbeing (e.g., higher interest rates when applying for a car loan).

API standards

Free access to APIs does not provide the right incentives to market actors. For open banking to flourish it is important to have an economic incentive/business model so industry players can continue to invest in innovation and constantly improve the security of the ecosystem. Under PSD2, ASPSPs need to invest into APIs to provide data access free of charge. This creates additional compliance costs for ASPSPs and regulatory asymmetry with respect to TPPs (see previous section on data sharing where this topic is discussed in detail).

Lack of incentives and enforcement, together with broadly defined regulatory requirements, have led some banks to limit or at least complicate access to their data (Maus & Mannberg; 2019). As the regulatory technical standards (RTS) of PSD2 do not detail specific API standards (PSD2's open banking provisions set a performance criterion for APIs, but standards

[205] There are different consent models available for AIS services. The Berlin Group standard has determined them as the following: "Global Consent": TPP requests access to all accounts of a PSU. No IBANs have to be specified by TPP. "Bank Offered Consent": TPPs don't have to specify IBANs. PSUs get to choose the accounts they want to grant the TPP access to themselves during the redirect flow. "Detailed Consent": TPPs have to specify each account that they want to request access to individually via the corresponding IBAN.

are left to industry), different initiatives emerged across the Member States and banks – see box below. Due to lack of standardisation, each bank in the EU may develop different API standards, with different ways of connecting. Lack of standardisation can impact the API quality and delivery cycles[206]. Furthermore, this means also that TPPs need to develop separate solutions to access APIs of different banks. Thus, TPPs struggle to keep up with this proliferation (Maus & Mannberg 2019; Bijlsma et al. (2020). According to TPPs interviewed, the PSD2 model of XS2A via API model has enabled many new companies to enter the market[207], but implementation by the EU banks has mostly been poor (with very few exceptions), with a significant number of obstacles built in. The APIs vary greatly from bank to bank, despite the fact that they sometimes claim to use the same standard. Furthermore, they often do not work properly. For example, TPPs reportedly often do not receive the correct status feedback for scheduled PISP payments. The availability of APIs remains patchy, the scope of the data being accessed remains unclear and the reliability of eIDAS certifications is inconsistent across the EU. This has resulted in increased costs and resources, with obstacles remaining to the seamless provision of open banking services across the EU. Moreover, some stakeholders report that although there is an increase in APIs usage, a number of TPPs continue to work with screen-scraping due to the perceived limited data accessible through APIs.

Development of API standards within the EU: There is a lot of fragmentation arising from multiple API standards and differences in application of standards.

Existing approaches in the industry show that open banking is still in the early stages of development in most of the Member States. Although in some Member States domestic API standards have been established, cross-border interoperability in terms of access to data remains low, with most banks creating their own standards (The Economist, 2020).

France is one of the European countries, which has launched country-level harmonised API standards to grant access to payment accounts. The API standards in France have been implemented by the country's six major banks[208] and through their jointly-owned processing company, STET (Rolfe et al., 2021)). However, foreign banks operating in France, such as ING, adopted their own API standards.

Starting in 2004, German banks have been using HBCI/FinTS API standards[209] (Homebanking Computer Interface/Financial Transaction Services, a non-PSD2-compliant API) to grand access to third parties, mostly for account information services. HBCI/FinTS API standards are still the dominant access method in Germany. For connecting new and/or cross-border PISPs and AISPs, German banks mostly rely on NextGenPSD2 and NextGenMobileP2P standards, which were developed by the Berlin Group. The Berlin Group is a pan-European harmonised open API initiative. It currently has participation of 25 major stakeholders from 14 different Member States. Foreign banks' branches and subsidiaries in Germany usually opt to use the Open Banking API standards of their respective parent bank group.

In Spain and Italy, API access to most banks is outsourced; Spanish account aggregator Redsys provides open API standards in Spain, which are based on the Berlin Group's NextGenPSD2 standards, and in Italy, open API standards are provided by multiple account aggregators such as NEXI, SIA, and CBI Global (Rolfe et al., 2021). In Portugal,

[206] Well performing APIs (in terms of reliability and functioning) are essential to initiate payments, but also to provide a good customer journey.

[207] In terms of competition, a 2020 study shows that the payments-oriented FinTech sector in Europe has grown significantly after the implementation of PSD2. There are now more than 300 businesses in the EEA that are authorised to provide AIS and PIS. Source: Michał Polasik, Agnieszka Huterska, Rehan Iftikhar, Štěpán Mikula (2020) The impact of Payment Services Directive 2 on the PayTech sector development in Europe, Journal of Economic Behavior & Organization,Volume 178, 2020,Pages 385-401.

[208] BNP Paribas, Crédit Agricole, BPCE, Crédit Mutuel, Société Générale and HSBC.

[209] For further information see https://www.hbci-zka.de/

most banks perform highly on providing access to TPPs. SIBS, the local payment processor in Portugal, launched an API platform that gives TPPs access to 95% of bank accounts by bringing together 24 financial institutions.

Although most Danish and Swedish banks have an open banking strategy, implementation of standards remains fragmented, and functionality is often limited to displaying transaction and account information (Rolfe et al., 2021). In Denmark, Danske Bank uses the UK Open Banking API standards, Nordea use their proprietary API standard, and most other Danish banks rely on the Berlin Group's NextGenPSD2 API standards. In Sweden, banks often provide API access in combination with aggregators such as Tink, Open Payments and Meniga.

The situation is said to be particularly difficult situation for TPPs which existed before PSD2 and which were forced to change their existing (and well-working) "direct access" technology to "low-quality, low-performing API implementations". Consequently, existing PISPs and AISPs (pre-PSD2) faced high costs for implementing new API technologies; high costs of maintaining legacy technologies due to APIs not working properly; uncertainty costs due to complex and unclear legislation; increased friction leading to lower conversion rates due to poor redirections; increased risk due to reduced data access, which disabled non-execution risk mitigation and licensing burden. For new TPPs, new API technologies are not sufficiently well implemented and maintained by ASPSPs and alternative access is too costly to develop.

From PSPs' perspective, they have experienced additional burdens and resource investments in supporting integration requests and technical issues from TPPs using issuers' APIs. Fast-evolving technology also requires continual maintenance and further development of APIs on the issuers' side, which is not always proportional to returns. Finally, card issuers highlighted that the open APIs might provide opportunities for cybercriminals to access critical functionalities and sensitive customer data, thereby increasing cyberattack risks and issues.

There is lack of unanimity among market players for a single EU-wide API standard. Currently, there are several standards (and variations) across the EU such as NextGenPSD2 (a coalition of EU banks called the Berlin Group) or STET (France) – see box for an overview. Several stakeholders including industry associations are not in favour of a unique API standard that is prescribed by EU legislation offering the following arguments:

- Standardisation could hinder and slow down innovation. This could be because ASPSPs may decide not to include new functionalities, features or data, even upon TPPs request, because ASPSP may instead require that a certain use case must first be included in the API standard in order for it to be implemented in their interface. There are initiatives to extend standards with premium API features, so the ASPSPs' APIs can be used beyond what is offered in PSD2. However, others have stuck, so far, with the minimalistic approach of only including what is in scope of PSD2.
- The reason for poor APIs is because there is no incentive for banks to invest in well performing APIs; it is not because of lack of standardised API. Poor implementation of API standards is the problem; a single standard could still lead to bad implementation.
- It is "too late" to develop a single standard. It would have helped roll out PSD2, if a very clear set of technical standards and API had been launched. Currently there are several competing standards, but not a definitive one. This has slowed progress but not blocked it. Choosing now a single standard would make everyone abandon their solutions in order to adapt to it. So a unique standard would only help newcomers.
- It would hinder market efforts. Currently, banks adopt one of the available standards (normally, the Berlin Group in the EU) and apply their modifications within these standards: this means that TPPs have to make a lot of connections to different variants of API. Thus aggregators of APIs have emerged, allowing TPPs to access only a few aggregators facilitating this exchange. Some stakeholders acknowledge that a single API standard would have some advantages in theory. But in practice, even with a single standard, there would still be significant differences between the implementation of each

bank, so that a single standard would not be the solution. Several market players (ASPSPs and TPPs alike) are advocating for an industry-led, commercial approach, which uses premium APIs[210] that will allow competition for services going beyond the scope of PSD 2.

- Setting up the API specifications based on the legal framework should be left to the market. Changing the current principle to one mandatory standard would require again significant investment efforts for ASPSPs that do not yet use the defined standard.

Some stakeholders called for clearer standards rather than a single standard. Not having a clear standard gives latitude to AISP to create challenges to ASPSPs. One ASPSP explained that AISPs have complained that the ASPSP was not making itself open, while continuing to scrape because they want to access a much fuller data set than what PSD2 requires. Providing clearer standards that all market participants operate around will help mitigate scraping. This would also create further opportunities for innovation and competition between the various standards.

The evidence from the survey diverges from the interviews. In the survey, stakeholders were asked if only one global API standard would be fit to facilitate payments, more than half of the respondents (36 out 62) expressed a strong view that this should be the case. In fact only nine seemed to be against this statement, while the remaining 17 responses showed no relative opinion. Those against a standardised API commented that API standardisation might be good to facilitate adoption, but it would hamper innovation. Considering other regulatory requirements and standards, such as SEPA ISO XML20022 standards, there are always different forms of implementation, especially from banks and thus give rise to changes in the same standard. Hence, the enforcement of one global API standard is questionable for retaining a degree of flexibility and innovation.

Those in favour of a global API claimed that a common and precise API with standard rules and interpretation including enrolment would be the best solution to solve the current issue with ASPSP specific interpretation and implementation. Standardisation of APIs would thus reduce uncertainty, complexity and costs. However, when imposing standardisation, a broader pan-European but also global view should be taken into consideration. It was also mentioned by a couple of stakeholders that having a single entity which would have the authority to issue binding regulations with regards to open banking operational matters, would be useful.

One of the proponents of a uniform API standard cited the UK experience as a demonstration of the benefits of a single implementation entity, i.e. the Open Banking Implementation Entity (OBIE) for developing common standards for the market. According to them, it has been much easier for payment providers to build viable open banking solutions in the UK as a result.

In the context of the above discussions, several stakeholders expressed their support for current developments such as the SEPA API Access (SPAA) scheme or the EPC SRTP. SPAA scheme will address several issues raised above. For example, it would allow for mutual benefit (this could be remuneration, or it could be a different data exchange).

Stakeholders are strongly in favour a technology neutral approach to legislation. One stakeholder explained that user interface technology is the most rapidly moving goal post in the industry. APIs are state of the art today for text-based data, but voice interfaces, augmented reality, virtual reality, metaverse interfaces will come rapidly. Several stakeholders requested that a balance be struck between standardisation and technological neutrality.

Concluding remarks

[210] Some API standards have been extended with so-called premium API standards so that they can be used beyond the scope of PSD2.

While PSD2 has laid the foundations for open banking/open finance in the EU, many of the expected benefits and its full potential has not been realised due to issues relating to:

(i) data access
(ii) data sharing
(iii) consent and data protection
(iv) Fragmentation of API standards.

The main issues are that the PSD2 does not incorporate an incentive mechanism for ASPSPs to invest in well-functioning APIs to provide access to customer data to TPPs.. This, they argue, amounts to an unfair and regulatory-driven competitive disadvantage.

Moreover, as the RTS do not detail specific API standards, this has led to the emergence of multiple API standards and differences in application of these standards across the industry leading to sub-optimal outcomes. This has resulted in increased costs and resources for the industry, with obstacles remaining to the seamless provision of open banking services across the EU.

While there is widespread agreement that PSD3 should provide sufficient incentives to the industry to move in the desired direction, there are mixed opinions on whether there should be a single EU-wide API standard.

5.3. Efficiency

The efficiency criterion examines the relationship between the time, human and financial resources required for the implementation of PSD2 as well as the positive and negative changes generated through the Directive. The evaluation examines four questions, in particular:

- Were there factors that influenced the costs and benefits of PSD2? If yes, what were these factors?
- Which, if any, specific provisions of PSD2 can be identified that make cost effectiveness more difficult and hamper the maximisation of the benefits? Are there any specific areas/elements with simplification potential and/ or the potential for removing (unnecessary/cumulative) burden? What scope is there to realise cost efficiencies via further simplification?
- What is the achieved simplification and improved efficiency of the EU intervention, including any reductions (savings) or increases in regulatory burdens compared to the point of comparison/baseline?
- Are there opportunities to further simplify the legislation or to reduce unnecessary/disproportionate costs and complexities without undermining the intended objectives of PSD2?

The analysis builds on the results of the cost-benefit analysis and stakeholder consultation conducted as part of this evaluation, as well as a review of the relevant literature. The currently available evidence on the costs and benefits of PSD2 is scarce and the literature generally considers the expected impacts rather than providing actual costs/benefits or specific estimates. Stakeholder feedback is largely focused on early-stage effects. This comes as no surprise given that these impacts are only now becoming visible due to late Member State transposition. Consequently, the longer-term effects can still only be assumed. Another caveat to be noted is that costs and benefits differ across Member States and can be specific to each stakeholder. However, the evidence emerging from studies and, more recently, surveys can provide an indication of the most critical items that constitute the bulk of costs resulting from the implementation of the Directive.

A more detailed table with the costs and benefits assessed under this evaluation can be found in Annex 10, while Annex 8 provides an explanation of the assumptions and calculations behind the different cost and benefit items.

5.3.1. Main factors influencing costs

Based on the evidence gathered through literature, interviews and survey responses, and the estimates produced by this evaluation, the largest cost items linked to PSD2 are:

- Open banking, and in particular API-development
- SCA rollout, notably implementation costs and an increase in transaction failure rates
- Legal interpretation and uncertainty

The table below presents the results of the cost assessment exercise.

Table 9 Costs linked to PSD2[211]

Cost item	Stakeholders included in calculation	Value (if relevant, year)	Type
Development of application programming interfaces	Credit institutions	€2,200,000,000	One-off
SCA implementation	Credit institutions, TPPs, merchants	€5,000,000,000	One-off
Development of products based on APIs	TPPs	€140,000,000 to €285,000,000	One-off
Business loss due to SCA implementation (friction and complexity of authentication method)	Merchants	~ €33,500,000,000	One-off
Registration costs for new TPPs	TPPs	€10,000,000	One-off
Maintaining legacy technologies due to APIs not working properly	TPPs	~ €140,000,000	One-off
Increased uncertainty about processing of payments	TPPs	Too early to call	One-off
Bank API maintenance	Credit institutions	~ €278,000,000	Recurring
Maintenance of API-based products	TPPs	€53,000,000	Recurring
Informing consumers about rights and obligations, improving financial knowledge necessary for PSD2-linked services	Credit institutions	€123,000,000	Recurring
Ongoing supervision fees for new TPPs	TPPs	€3,000,000	Recurring
Higher need for supervision in national administrations due to PSD2	National administrations	~ €30,000,000	Recurring

[211] Note that one of the reasons for the different range of estimates is related to the different population sizes of affected stakeholders. The calculations relate to 1125 credit institutions and banking groups/associations and 189 TPPs. The calculations and estimates for sub-groups within these populations are provided in the relevant methodological Annex.
In addition, assumptions and limitations behind the estimates presented in the Annex provide important caveats that nuance the accuracy of the estimates.

Cost item	Stakeholders included in calculation	Value (if relevant, year)	**Type**
Reduced revenue in acquiring and issuing cards	Card schemes	Too early to call	Recurring
Less room to steer consumers to cheaper means of payment (surcharge ban)	Merchants	Too early to call	Recurring

Source: own estimates

A number of studies surveying the payments industry (e.g., Deloitte, 2017, Polasik et al., 2020 or Tink, 2020) indicate a considerable importance of the costs associated with the implementation of PSD2. Emphasis of the impact from different elements of the Directive varies considerably across stakeholder groups. For instance, the consulted merchants and business associations report that the costs associated with payment services are not clearly distinguishable to them from aggregate costs requested by their technical service providers, and therefore some of most cost-heavy elements of PSD2 do not feature prominently in the replies of this stakeholder category.

Moreover, the assessments and views from the stakeholder consultation differ from the overall relatively balanced picture reported throughout the literature. For instance, the overwhelming majority of consulted banks and associations have indicated that costs largely outweigh benefits. National authorities and payment institutions (TPPs) established before PSD2 was introduced were more positive about the general impact but tended to agree with the overall negative assessment. While these perceptions are largely in line with the estimates produced for this evaluation, it should be noted that given late national transposition and unpreparedness for applying certain aspects of the legislation by the initially set deadlines (e.g., SCA rollout), potential benefits might take longer to materialise.

Open banking and investments in IT infrastructure linked to API deployment are considered as some of the most sizeable PSD2-related costs. The evaluation estimates a cost of EUR 2.2bn incurred by credit institutions for the implementation of APIs allowing TPP access. This estimate includes all IT related costs to comply with the Directive, including development costs of APIs and update of legacy infrastructures. It assumes that, due to the high level of investment required, only some of the largest ASPSPs have engaged in the development of their own APIs, with many instead opting for providing access by making use of a provider's platform developed either in collaboration with or by other market players (i.e. outsourcing). However, even in these cases a potentially costly optimisation of inhouse process flows had to be undertaken, including but not limited to the costs linked to the interactions with TPPs. These sunk costs are likely to have been recouped already, through higher fees on other products, efficiency of operating the new infrastructures or revenues on premium APIs.

Already around the time of the adoption of the Directive, ageing core IT systems in use by a significant number of banks were considered to inhibit further technological innovation in the sector (EBA, 2016). The update of legacy infrastructures in response to PSD2 was expected to almost double investments in 2017 in comparison to the preceding years (Romanova et al., 2018). A survey conducted in 2020 by Tink, an open banking platform, clearly shows a continuation, and even an acceleration of the trend. The responses, based on answers from 290 financial executives of financial institutions in 10 EU countries, Norway and the UK, offer an overview of the scale of investment going into open banking. The median spend of the firms surveyed was between EUR 50m and EUR 100m, but 45% indicated that their budgets exceed EUR 100m. These figures should be taken with a degree of caution, as they might be biased upwards. The largest chunk (28.3%) went to IT-related investments. This entailed modernisation of the technology stack for dedicated interfaces under PSD2, API gateways, improvement of the security framework and cloud computing.

A 2017 Deloitte survey found that more than two-thirds of the respondents were already engaged in some sort of collaboration related to the provisioning of APIs to define a collective approach to third party access standards. An attempt to make use of economies of scale through collaboration on APIs was also reported by industry representatives, though as noted under other sections there are several standards and API platforms in operation across different Member States. Common APIs (e.g., in Portugal) offer opportunities for reducing the cost of API development. While this has undoubtedly led to savings, interviewed banks unanimously reported high expenditure in this area.

In addition to one-off development costs, ASPSPs incur maintenance costs for their APIs. These include gateway maintenance, ensuring server availability, managing potentially high traffic volumes, etc. The estimate of EUR ~280m recurring annual cost is based on the latest available data and is likely to increase with the growing number of API calls across the EU (but making use of economies of scale).[212]

The rise of 'premium APIs' reported on in preceding chapters provides a partial response to the above cost factors. While charging for API services generally entails expected return on development costs and any maintenance cost incurred, ASPSPs cannot charge for the provision of these APIs. Credit institutions can compensate for them through price increases on other services (e.g., account maintenance fees) or the provision of additional data through APIs not mandated by PSD2 but making use of the infrastructures developed to comply with the directive. However, it presents an additional cost to TPPs that might need access to additional data to offer these services in sufficiently high quality to their customers. An example of such an issue was reported by a payment institution interviewed, which claimed that information provided by ASPSPs is not always sufficiently clear. This can potentially lead to payment cancelations or the need to verify recipients – both of which incurs extra costs (e.g., time investment or customer loss).

Some of the banks interviewed for this study reported limited uptake of their PSD2 API services, noting that some TPPs continue to use screen scraping to have access to the same services as before. TPPs, on the other end, noted that banks were slow in providing standard API connections to open banking data, and reported poor implementation. Some respondents suggested that one reason could be that banks prefer to limit access to fend off increased competition by FinTech companies they perceive as a threat to their business model (PISs competing directly with credit cards).

The above proves especially problematic to PISPs created after the introduction of PSD2 and which are consequently not well-established players on the market. New PISPs, which constitute one of the main targets of the Directive, unanimously listed considerable obstacles for market entry and growth. Besides general issues with access to payment accounts data, the main problems relate to a disproportionate administrative burden on reporting, licensing and other compliance requirements. The evaluation estimated EUR 10 million in registration costs between 2018 and 2021 for new TPPs. Ongoing supervision costs for all TPPs (old and new) amount to a minimum of EUR 3m each year. In addition, the study estimates a one-off cost of ~ EUR 140m for maintaining legacy technologies to access account information, for instance screen scraping. With API availability greatly improving already in 2021 and integration becoming easier (Salt Edge, 2021), accessing these services is likely to become easier. Therefore, this cost is assumed only for the first three years of implementation (hence it is a one-off). The reduction of associated costs could generate further uptake of open banking APIs.

Another cost category identified by this evaluation relates to the development and maintenance costs of products based on APIs. This relates primarily to the products developed based on ASPSP PSD2 APIs mainly by TPPs[213]. These products offer – among others – opportunities for

[212] See for instance the analysis of TPP registration data, as well as API calls by Konsentus, 2021 here
[213] While banks develop such products as well, they go beyond PSD2 requirements, and therefore are not within the scope of the evaluation.

improved financial decision-making, broader payments choice or better borrowing. Upfront investment costs, at EUR 285m, are estimated to be relatively high. However, they often constitute the core of the respective TPP's businesses, and the need for large upfront investments are not uncommon in the FinTech industry. This is somewhat similar to the ASPSP need to invest in IT. Annual maintenance costs are estimated to be around EUR 53m.

Costs and benefits related to strong customer authentication make up another important group relevant to overall PSD2 CBA. With still 41% of merchants citing fraud and cyber risk as their top concern in 2022 according to a Checkout.com survey, SCA implementation is indeed a critical part of the overall benefits to be offered under PSD2.

Costs associated with the implementation of SCA (~ EUR 5bn) feature prominently in the stakeholder data collected for this assignment across a diverse set of stakeholders that includes banks, payment institutions, merchants and national authorities.

Many banks and (larger) merchants – especially in countries with well-developed markets – considered that their systems were already of sufficiently high quality to ensure secure transactions and the introduction of new requirements called for considerable investments. For instance, this entailed a change in communication protocols for authenticating cards and merchants, as well as additional efforts to ensure that the impact on clients is minimised.

Respondents were far from unanimous in their judgement of the extent to which the implementation of SCA will bring the expected benefits in fraud reduction. Sceptics cited the inefficiency of mandating the use of a specific technology with other, potentially less costly options available to banks. This could be somewhat inefficient in a market that is experiencing rapid development that could render current solutions obsolete even in the short term.

Much of the benefits brought about by more secure transactions could be undermined by the increased friction leading to customers – particularly less tech-savvy ones – abandoning transactions and thus lower conversion rates. As a result, merchants risk losing a considerable part of their revenues to such issues. This is especially problematic for smaller entities, which could struggle to cope with a sizeable chunk of their revenue stream continuously being at risk.

The business lost to SCA implementation is the largest cost estimate of the CBA analysis in terms of value. A 2020 report by CMSPI, an advisory firm, estimated that failure rates could range from 25% to as high as 59% across the EU, putting overall EUR 108.099bn of transactions at risk in 2021 alone. A follow-up report found an average European failure rate of 30% in March 2021. These figures are generally in line with the numbers reported by the stakeholders consulted. However, they relate to the gross dropout rate, which does not necessarily coincide with unique attempts to carry out these transactions – consumers are likely to use different payment means before eventually abandoning a purchase. Therefore, the actual value of failed transactions is likely to be considerably lower. With an assumed failure rate of 14.8% in 2020 and 5% in 2021, the estimate provided by this evaluation stands at EUR 33.5bn. This, however, still probably overestimates the actual impact. Consumers are likely to opt for another merchant to carry out their purchase after several failed attempts rather than completely abandoning it. This would not be accounted for even in the net dropout rate figure used for the calculation. With an increasing trend of online sales over the 2020-21 period in the EU, the evidence to suggest a failure rate in the range suggested by available literature is thin.

Moreover, the estimate is for the two years following SCA implementation. This is because there are reports suggesting that the initially high dropout rates could be reduced over the longer run. Reductions are expected from better informed businesses making more use of the SCA exemptions, as well as the latest 3DS enhancements. In particular, the new 3DS2 protocols make it possible for users to take advantage of more intuitive authentication methods through biometric data such a fingerprints or facial recognition (Kania, 2022).

Using the Transaction Risk Analysis (TRA) exemptions is an example of optimising the use of SCA. TRA makes is possible to offer merchant acquirers higher thresholds for SCA-exempted

payments. The thresholds depend on the average fraud rate of the merchant acquirers, with lower rates enabling higher transaction thresholds. With higher thresholds, SCA exempted payments could lead to lower failure rates, and thus less revenue foregone. However, given that ultimately fraud rates depend on merchants, not merchant acquirers, one of the payment institutions interviewed reportedly decided to set up a second (with a view for a potential third) legal entity to be able to cater to the needs of different groups of merchants. While this is likely to considerably reduce failure rates, the costs of setting up a legal entity are very large in terms of the time, human and financial resources required.

Although no figures could be estimated for this item due to insufficient evidence on actual values, legal costs are another item reported to be substantial. In particular, these stem from uncertainty from the application of certain provisions, unclear definitions of the negative scope and the differences in the interpretation of the directive across Member States. Legal ambiguity was picked up by competent authorities in the consultation sample. The complexity of supervision is reported to have increased considerably, with new tasks, conflicting interpretations and the immediacy of responses all considerably challenging authorities. This is captured by the cost estimated for national authorities linked to the increased need for supervision (EUR 30m), though this is generally borne by the industry, for instance through the ongoing supervision and registration fees estimated for TPPs. The interpretation of the scope of payment services excluded activities as well as interaction with other EU legislation (e.g., EMD2 or GDPR, see section on coherence) and has required considerable effort from competent authorities. While EBA work on Q&A is considered helpful in facilitating this process, there are still outstanding aspects that remain ambiguous, which also lead to the abovementioned divergence in implementation across Member States. In the case of banks, this divergence constitutes a major obstacle and prevents them from rolling out a single solution across their markets. Instead, account data access must be tailored on a country-by-country basis. Finally, payment institutions, particularly smaller ones lament the lack of clear guidance and sufficient differentiation between firms of different sizes that lead to disproportionate costs compared to larger competitors and banks.

A sizeable cost item (a rough estimate amounts to ~ EUR 123m) reported on by banks is linked to the provision of information and explanations related to the application of PSD2. This includes, for instance, making clear how TPP services differ from those offered by the bank itself, which were not intuitive for a large part of their clientele. A payment institution interviewed also reported that the general lack of financial education of consumers creates a considerable bottleneck to the uptake of PSD2 benefits and therefore affects the overall efficiency of PSD2. The major problems relate to understanding how customer payments and accounts are secured, but also general knowledge about open banking as a concept. According to the interviewee, stakeholders are not sufficiently incentivised to provide this education, leading to lower uptake of PSD2-enabled services.

Finally, the ban on surcharges seems to constitute an important element that hampers the cost effectiveness of the Directive from the point of view of merchants and business associations. Stakeholders report that preventing merchants from offering different payment methods at different prices leads to a distortion of price signals towards the customers, which distorts the market. It makes it equally impossible to steer consumers to methods that have a lower risk of fraud, leading to further potential losses.

5.3.2. Main benefits and improved efficiency of the intervention

The results of the evaluation indicate that the main benefits linked to PSD2 are:

- Improvement of the functioning of the Single Market (including increased market access for TPPs)
- Unlocking the potential for innovation
- More secure payment environment for customers and a reduction in fraud rates

As already noted in the introduction to this criterion, the cost-benefit balance is somewhat cost-heavy given the relatively recent (and late) transposition of the Directive by Member States. Consequently, some benefits are still difficult to quantify (noted as too early to call) while others are likely considerably understated.

With this in mind, the key benefits associated with PSD2 found in the publicly available literature are generally echoed by the answers collected through the stakeholder consultation for this study. Building on this data, the estimates produced by this evaluation are summarised in the table below.

Table 10 Benefits linked to PSD2[214]

Benefit item	Stakeholders included in calculation	Value (if relevant, year based on)	Type
Increased market access	TPPs	€1,600,000,000 (2020)	Recurring
	Credit institutions	Too early to call	Recurring
Reduction in fraud thanks to improved customer protection measures	Consumers	~ €900,000,000 (2020)	Recurring
Efficiency of operating new infrastructures	Credit institutions	Min. €21,000,000	Recurring
More competitive pricing for payment services	Merchants, consumers	Too early to call	Recurring
Benefits of new products based on PSD2-enabled APIs	TPPs, credit institutions, consumers	Too early to call	Recurring

Source: own estimates

The surveys referred to under the previous section also take note of the abovementioned benefits. For instance, the respondents to Romanova et al., 2018 expected a positive impact on overall competitiveness resulting from PSD2. In particular, the new legislation was seen to promote the use of technology creating a drive for innovation and regeneration of service channels. The Roland Berger survey also (Maus & Mannberg, 2019) takes note of key opportunities – benefits – associated with PSD2. Actors on the payments market, and banks in particular, expect that large upfront investments in IT and APIs will have clear long-term benefits. The increased use of APIs, modernisation of IT infrastructure and ensuing internal process optimisation could help standardise information exchange along predefined data points even between non-harmonised systems. This is also in line with global trends. A 2020 McKinsey survey found that banks increasingly rely on internal APIs to reduce costs and complexity associated with IT integration. While the data provided by stakeholders on this aspect is very limited, we estimate a minimum of EUR 21m in savings linked to more efficiency gained through new infrastructures. While actual savings are difficult to quantify, this figure is likely to be substantially higher.

Moreover, open banking allows for the marketing of high-end products on the platforms of competitors, thereby offering the possibility to reach new potential clients and create additional revenue streams. A report[215] by Allied Market Research valued the European open banking market at EUR 5.4bn, though this estimate includes the UK, which could make up more than half of this figure. The report forecasts a CAGR of 23.18% until 2030, resulting in an eightfold increase over the next decade. Therefore, these benefits could also be substantial.

[214] See note on population size and caveats under the table summarising costs
[215] Available here

By becoming TPPs, banks could get access to a more comprehensive dataset on their clients, allowing for more targeted advertising, the improvement of scoring models or a simplification of background checks. While this option seems to offer clear benefits, based on the evidence presented above this does not seem to be currently in the focus of banks. From the point of view of customers, new personal finance management tools could lead to saving time on household administration.

Some of the banks interviewed highlighted that PSD2 has undoubtedly brought benefits to the EU payments market, which are very much in line with the above survey results. These generally relate to the creation of common rules that allow services to be offered across country borders, with an overall stability that allowed for the development of the sector. However, these banks also reported that other regions, even in the absence of much regulatory intervention, are experiencing a similar innovative boom. Put in this perspective, the respondents believe that legal certainty was important to encourage additional investments that might not have materialised in a more fragmented and unclear environment, but the extent of contribution remains unclear to them. Another benefit cited is linked to the possibility to offer new FinTech products and propositions to customers.

Payment institutions created before the adoption of PSD2, especially smaller ones, were very positive about the impact of the Directive on improving competition on the internal market, as well as unlocking the potential of open banking. They consider PSD2 to be a major step forward for the industry as it created and structured the rules for non-banking entities. In doing so, it allowed for more companies to compete with banks at different levels, including in the provision of accounts, cards, payment services, thus giving consumers and businesses more choice in the financial products they have access to. PIs created after 2015, as noted under the section on costs, are generally more negative about the cost-benefit balance. However, they also see a considerable benefit in opening up the possibility of TPPs to enter the regulated field. Along with the general literature and stakeholder assessments, the results of the CBA exercise for this evaluation also indicate that with relatively large upfront (one-off) investments required by TPPs, the benefits are only slowly beginning to materialise. The evaluation estimates EUR 1.6bn in benefits of increased market access for TPPs, based on 2020 figures.

The ministries consulted generally took a balanced view on the different costs and benefits associated with PSD2. While it is too early to draw solid conclusions due to the small sample of ministries consulted, it seems the benefits are more visible to authorities operating in countries with payment markets that were less developed at the time of PSD2 adoption. The national authorities seemed well aware of the major cost items faced by market players. Respondents cited SCA implementation, API and IT infrastructure development, as well as costs linked to legal interpretation as the most salient ones. However, they also added that many of these are inherent features of legislative changes and also entail opportunities for innovation. Ministries perceived legal certainty and increased protection to consumers, as well as increased competition, as the most important benefits of the Directive. Competent authorities were generally more negative about the balance of cost and benefits than ministries. Some highlighted the increase in competition, especially regarding the entry of new PSPs in the regulated field as a result of more favourable conditions and progress in the integration of the Single Market.

Though as noted under the previous section, SCA rollout comes with high costs, it also seems to bring clear benefits in fraud reduction. The study estimates a yearly recurring benefit of ~ EUR 0.9bn thanks to the reduction in transaction fraud, based on data available in the literature.

For instance, a report by VISA found a 20% drop in fraud in the first four months of 2021, coinciding with the increasing adoption of 3DS across Europe. The preliminary observations on SCA-related fraud figures by the EBA also indicate a clearly positive impact. This is expected to bring about clear savings for both merchants and consumers. Several competent

authorities interviewed also observed a reduction in fraud thanks to the application of SCA measures.

A factor limiting the extent of these benefits is the still incomplete uptake of PSD2-enabled services to date. Benefits seem especially modest in markets that were already well-developed prior to the introduction of the Directive (e.g., the Netherlands). This observation is generally echoed by several stakeholder categories.

In line with the above, consumer organisations believed that one of the major benefits brought about by PSD2 is precisely its role in making the payment environment safer. However, as noted in the preceding section, these benefits are mostly concentrated at tech-savvy users, but many PSD2-mandated requirements make it harder for others, especially for older generations and persons living with disabilities to make use of payment services.

5.3.3. Opportunities for simplification and maximisation of benefits

Opportunities to simplify the level 1 legislation generally relate to the reduction of legal ambiguity, the large room for interpretation by NCAs leading to inconsistent application and improvement of the interplay of PSD2 with other legislation. Specific aspects related to level two, namely on the ’90-day rule’ and technology neutrality were also identified.

Stakeholder feedback was generally positive on the potential for simplification. Some stakeholders (around 20% in interviews and ~25% in the survey) stated that they had no opinion or provided no insight/reply regarding this question. Several (at least 6% in interviews and around 3% in the survey) explicitly claimed that there is no need to revise or simplify the legislation to reduce unnecessary costs or maximise benefits. The largest group (in the case of the survey, 71%) believed there is a potential to do so.

However, the results of the analysis of costs and benefits suggest that the most substantial items are sunk (one-off) costs that have already been incurred. Therefore, the potential for simplification is overall relatively modest. Some of the recurring costs examined by the evaluation (e.g., maintenance) would also be hard to lower. With the benefits only now becoming visible (see previous section), opportunities to maximise them remain unclear.

Stakeholder feedback on the potential for simplification or maximisation of benefits is in line with the outcomes of other evaluation criteria analysed and will therefore only be summarised to avoid duplication. The most important aspect relates to the inconsistencies in the application of the Directive, resulting from the large room for interpretation left to national authorities. This, as noted under the main factors influencing costs, creates issues for several stakeholder groups that require considerable investment (i.e. in time or legal costs). In addition, stakeholders would be in favour of a more technology-neutral legislation, a comment generally made for both APIs and SCA, which in their view would reduce burden. The ’90-day rule’ for re-authenticating AIS with ASPSPs was consistently reported by AISPs as being cumbersome. A more detail analysis of these issues is provided under the effectiveness criterion.

Another reported aspect linked to the simplification of the legislative landscape – analysed under coherence – relates to the improved interplay between PSD2 and other legislation, notably GDPR, AMLD and EMD2.

Several banks (at least 21 out of 43 interviewed, ~49%) suggested that article 65 on confirmation on the availability of funds be removed as they experience no or very little uptake of these services. While some evidence was provided to back up this statement, data to systematically assess the overall validity of this claim is not available, and therefore no definitive conclusion can be reached.

5.4. Coherence

Coherence analyses the extent to which the provisions of the PSD2 are aligned with one another (internal coherence) and with other interventions (external coherence). This chapter answers the following evaluation questions:

- To what extent are the provisions of PSD2 consistent with one another?
- To what extent are elements of PSD2 coherent with other EU policies and pieces of legislation, and particularly with other rules in the field of payments?
- How will PSD2 rules on operational and security risks interact with the rules in the Commission's regulation on digital operational resilience for the financial sector (DORA)?
- With regards to data protection, how do PSD2 provisions on access to payment accounts and the processing of personal data for payment purposes adhere to the GDPR and EDPB Guidelines? In particular, is there a need to further align and ensure complementarity and consistency between PSD2 and GDPR? In that respect, is there a need for a clarification regarding the basis for the processing of personal data for payment purposes?
- What, if any, specific inconsistencies and unjustified overlaps, obsolete provisions, gaps and/or synergies can be identified in relation to PSD2 and the other relevant EU legislation covered above? How do they affect the application/performance of these pieces of rules?
- Is there a need to incorporate rules laid down in Delegated Acts and further EBA guidance into a possible revision of PSD2 and vice versa? If so, which one(s) and at which level? If not, why?

The main information source for the coherence analysis were the texts of all relevant legislation, including soft law (Level 3) and relevant case law. The analysis was conducted through a legal assessment and interpretation in line with the guidelines of the Better Regulation methodology. Additional desk research was carried out to ensure that the analysis if based on a comprehensive set of available information. The analysis was limited by the scarcity of published research that is relevant to coherence. Stakeholder interviews did not feed significantly into the coherence chapter, mostly because stakeholders were unable to answer questions relevant to coherence to a sufficient level of detail. The majority of the findings in this chapter are therefore based on an in-depth expert analysis of the provisions of PSD2 and other legislation, in particular those applicable in the field of payment services.

5.4.1. To what extent are the provisions of PSD2 consistent with one another?

Overall, the PSD2 shows a fair degree of internal coherence. Indeed, one of the objectives of the first review of PSD was to ensure the internal coherence of the PSD2, i.e. that its provisions are not in conflict with one another, contradict one other or render one another impracticable. For instance, the rules and obligations set out by the PSD2 appear coherent when it comes to achieving its objective for transparency of conditions and information requirements for payment services, alongside establishing the respective rights and obligations of payment service users and payment service providers in relation to the provision of payment services in a way that fits the needs and expectations of all parties.

However, there is some evidence of incoherence when it comes to the implementation stage in Member States, where gold plating or interpretation issues have arisen in some areas and jurisdictions. While the resulting legal fragmentation can undermine the internal market objective of PSD2, the EBA was able to successfully address most coherence issues at implementation stage through its Q&As and GLs.

Specifically, Article 2 (Scope), Article 3 (Exclusions) and Article 4 (Definitions) have been the object of clarifications by EBA via Q&As following relevant questions raised by market participants that can form the basis of an improved and more precise wording within the forthcoming review of PSD2. Typical examples of such clarifications include: the definition of payment service, payment account, money remittance, unique identifier, remote

and non-remote payments, electronic payment transaction, acquiring of payment transactions, authentication of a transaction, payment initiation service, account information service, acquiring of payment transactions, payment instrument, agents and sensitive payment data, (see also chapter "Clarity of the definitions used in PSD2" for more detail).

Furthermore, questions about what might and might not qualify as a payment account or payment instrument under PSD2 were evaluated and interpreted by the CJEU in its rulings, most notably with the help of the judiciary, i.e., ECJ ruling in Case C-191/17[216] and Case C-616/11[217].

Ambiguity in terms of PSD2's fundamental concepts and exemptions and the subsequent heterogenous interpretation across the Member States bring about an uneven playing field and create an incentive for forum shopping.[218] New definitions (or even exclusions) might be also added as a result of the emergence of new types of payment services or providers (e.g., recognising the issuance of e-money as a payment service, or including crypto asset service providers to the scope).

Moreover, there is a need to ensure that the current PSD2 provisions remain coherent with the overarching objective to facilitate the emergence of a well-functioning payment services market, also in the face of technological development and market changes. This is particularly relevant when it comes to new types of payment services and technological possibilities (for instance, new types of players, such as TPPs, FAANGs,[219] FinTechs), as well as new EU initiatives such as open finance or the digital finance strategy. To address the shift from open banking to open finance, a regulatory action within the PSD2 needs to consider the current and near future trends in open finance While keeping the technology neutrality of the PSD regulatory framework.

In addition, with regard to the scope of PSD2 applicability, new 'white-label' business models, payment instruments with limited purposes, and especially technical services providers such as intermediaries in the payment chain (e.g., getaways and hubs, data processing and storage providers, RegTech companies for meeting regulatory compliance requirements, aggregators, SCA authentication providers, SaaS providers, and various IT maintenance providers in general) could potentially be added to the remit of the PSD, together with adequate obligations that are proportionate to the principle of a risk-based approach to a specific type of TSP.

The liability provisions under PSD2 can be divided into two: on one hand, there is the liability of the PSP with regards to the payment service user, and on the other hand, there is the liability among particular PSP actors:

- When it comes to payments service users, it is in line, in particular with consumer protection, that, except under abnormal and unforeseeable circumstances, the liability in respect of the execution of a payment transaction accepted from the payment service user (to some minor exceptions), is imposed on the PSP.
- Regarding PSPs, gold-plating and the resulting 'forum-shopping' can undermine a homogenous application and enforcement of requirements in the field of financial services. The consequences of differences in transposition across the Member States,

[216] The CJEU held that the concept of 'payment account' does not cover a savings account which allows for sums deposited without notice and from which payment and withdrawal transactions may be made solely by means of a current account., 2018. Available at: Case C-191/17 .

[217] In which the CJEU elaborated on the concept of 'payment instrument', 2014. Available at: Case C-616/11.

[218] For instance, in a Member State an entity is refused for authorisation as a business activity pursued is considered as being within the exemptions under Article 3 of PSD2, whereas in other Member State the same entity is authorised, as the same business activity is considered as being a payment service which is not exempted under Article 3 of PSD2.

[219] 'FAANG' stands for Facebook (currently Meta), Amazon, Apple, Netflix and Google (currently Alphabet).

with a special view to the liability, is evidenced, for example, in relation to the liability for unauthorised transactions.[220].

5.4.2. To what extent are elements of PSD2 coherent with other EU policies and pieces of legislation, and particularly with other rules in the field of payments?

EMD2

The EMD2 has been in force for over a decade and after the implementation of PSD2, the two regimes converged, but remained separate.

At present, the differences between the services provided by payment institutions and e-money institutions (i.e., mainly EMIs providing payment services connected solely to the issuance and distribution of e-money) no longer seem to justify a distinct authorisation and supervision regime and these could instead be brought under a single framework. This is especially the case where business models are very similar and from the customer perspective perceived also similarly.

More clarity and a systematic overview of "one payment services and electronic money ecosystem" should be considered as the main goal of a merger.[221] For instance, a merger could eliminate unnecessary overlaps (e-money account and bank account definition, capital requirement rules), redundant provisions (customer protection rules according to different standards in each of the framework, general prudential rules), and potential conflicts (e.g., e-money issuance not being a payment service per se, KYC obligations). Possible negatives of a merger are more marginal, like for instance a perceived lack of clarity of provisions formerly applicable in the EMD domain in a merged intervention.

As the respective scopes of PSD2 and EMD2 exclude certain services and instruments, it is important to ensure that any exemptions granted to businesses posing low risks remain justified. In this regard, in case of a merger, the interplay between PSD2 and EMD2 (Article 1 of EMD2) needs to be duly addressed in the reviewed PSD2.

Supervision and oversight of the relevant actors in the payments chain has become increasingly complex, considering the emergence of many new business models and group structures. Of particular concern are payment conglomerates including both regulated and unregulated entities. In this context, problems encountered by unregulated entities providing technical services to support some of the group's affiliates (e.g., technical service providers providing services to regulated PSPs) could potentially have a spill-over effect. Making use of ICT services is symptomatic for operations of the PSPs, whereby those services, due to their specific nature, are provided by unregulated technical service providers, regularly as [third-party] outsourcing. The portion of ancillary technical services is even higher in the context of services under EMD2. Because of the similar subject and presumed alignment of PSD2 and EMD2, the requirements governing the use of ancillary technical services should be developed in accordance; in this regard, activities of EMD2 entities (or their group affiliates) under Article 6 of EMD2 should be duly checked with regards to the provisions concerning operational and security risks in Article 95 of PSD2, respectively Article 19(6) of PSD2 concerning outsourcing. From a broader perspective, the decision on the shift from currently unregulated technical services providers to become subject to regulation should be discussed with the respective ESAs (and indirectly with the NCAs).

[220] More details are available in EBA's Discussion paper on preliminary observations on selected payment fraud data under PSD2, as reported by the industry.

[221] E-money is no longer used only in closed-loop ecosystems. They are transferred through payment systems to accounts which are not necessary e-money accounts. When e-money are transferred to other PSPs or are used to make card payments, the issuing and redemption of e-money make no sense in such cases.

SFD (Settlement Finality Directive)

In order to enhance the open and accessible payment ecosystem, the SFD should be extended to EMIs and PIS.[222] Currently, there is an ongoing review of the SFD framework addressing this very purpose,[223] where it is being considered to extend the scope of the SFD to include e-money and payment institutions.

Access to payment systems is essential for effective competition and innovation in the payment systems market. As payment and e-money institutions compete with banks to provide payment services and contribute to innovation in the payments market, it is important to guarantee that all players have fair, open and transparent access to payment systems. Concerning PSD2, the access is granted in Article 35(1) of PSD2.

In this context, securing the right of access, under fair, reasonable and non-discriminatory conditions, to technical infrastructures that are considered necessary to support the provision of payment services, will need legislative action,[224] in the form of a revision of the SFD framework (and not the PSD2 review).

AMLDV

AML/CFT rules play a vital role in the infrastructure of payment services governed by the PSD2, to which the AMLDV is complementary, but from the perspective of coherence quite independent. In this regard, all PSPs are governed by the AML framework.

Nevertheless, **in ensuring the coherence between the PSD and AMLD, it is crucial to follow up and build on the work conducted by EBA,** which identified and addressed relevant issues in the interplay between PSD2 and AMLD (see especially revised EBA GLs on risk factors - EBA/GL/2021/02).

Without prejudice to the above, and exclusively with a view to ensuring clarity in the wording of PSD2 provisions, attention may be drawn to Article 33(1) of PSD2. This provision expressly exempts the AISPs from complying with AML requirements, although, the AISPs must comply with the AML framework, as they fall within the definition of obliged entities under the AMLD. Therefore, the wording of Article 33(1) of PSD2 should be adjusted so that the necessity to comply with AML requirements for the AISPs flows directly from PSD2 and not only from AMLD.

Fund Transfer Regulation (FTR2, also known as Wire Transfer Regulation - WTR2)

FTR2 have broadened the regulatory requirements already present in the FTR1 around the information relating to payers and payees that must accompany a transfer of funds, sent or received in any currency, when either the payer's or payee's PSP, or an intermediary PSP, is established in the EU or the EEA. Although the FTR2 is not (inter)dependent on the AMLD, both pieces of legislation follow the same effort to crack down on global illicit financial flows present in the EU. The main purpose of the FTR is to ensure traceability of payment transactions, which gives the PSPs and regulators (FIUs, NCAs) a powerful tool in the prevention, detection and investigation of money laundering and terrorist financing.

On introduction of the FTR2 there was substantial room for interpretation, as it did not set out in detail what PSPs should do in a practical manner to comply with the high-level rules. The issue was the lack of clarity vis-à-vis the requirements, which led to different interpretations and to disruptions of payment flows and unintended breaches of the FTR, as well as a fragmentation of the regulatory landscape. However, none of those issues need to be

[222] European FinTech Association, "EFA Position Paper on the Settlement Finality Directive Review", 2021 .

[223] Financial Stability Board, 'G20 Roadmap for Enhancing Cross-border Payments. First consolidated progress report', 2021.

[224] DLA Piper, "EU Retail Payments Strategy – the journey continues: Conclusions adopted by Council of EU", 2021.

addressed within the PSD2 revision, as those obstacles have already been resolved by the issuance of ESAs guidelines.

FTR lays down rules on the information on payers and payees, accompanying transfers of funds, in any currency, for the purposes of preventing, detecting and investigating money laundering and terrorist financing. Thus, the FTR interacts, in particular, with both PSD2 as well as AMLD. In this regard, FTR extends the liability of the PSP when providing payment services, whereby the PSP is obliged to carry out additional checks (a name-number-check) in respect of information to be used in a payment transfer. Although further clarification would be beneficial regarding the scenario in which such a check is mandatory, but may be replaced by previous fulfilment of AMLD obligation, that clarification is out of the scope of the PSD2 revision (it may be addressed, for instance, by EBA's Q&As).

Further clarification, but again in EBAs guidelines (no within the PSD2 review), may be recommended in respect of the detection requirements and handling of transfers with missing information (Article 7, 8, 11 and 12 of FTR2) and suspicious activities assessment and reporting (Article 9 and 13 of FTR2).[225]

FTR2 lays down a list of information to be part of a payment. However, also other information, such as alias or proxy may be part of a payment order, whereby proposals for using alias or proxy for making a payment transfer occurred.[226] In this regard, both FTR2 as well as PSD2 imply that only the IBAN is the basis for a payment transfer, while alias or proxy may accompany the information in a payment order, but only as additional information. This is also in line with the PSD2's provision on liability (Article 88(5) of PSD2) providing for that where a payment order as added with alias or proxy along with the IBAN, the PSP is liable only for a payment transfer made in accordance with the IBAN. Hence, there is no incoherence between FTR2 and PSD2 regarding this issue, and no legislative action towards PSD2 within the review is needed.

eIDAS

In the context of the Digital Identity for all Europeans initiative, the Commission has introduced an action to establish a European Digital Identity Wallet. The aim is to establish a framework/tool available to EU citizens, residents and businesses that want to identify themselves or provide confirmation of certain personal information, that can be used for both online and offline public and private services across the EU.[227]

As it is expected to be widely applicable, the European Digital Identity Wallet may be used within the provision of payment services under PSD2, including the SCA. However, while a proposal,[228] including the introduction of the European Digital Identity Wallet, has already been developed, it is not clear when the updated framework will take effect. In addition, the use of the European Digital Identity Wallet is foreseen as being voluntary for users. Hence, information on the current interplay between eIDAS and PSD2 is provided below.

eIDAS complements PSD2 by providing a 'tool' – the eIDAS certificates, namely the qualified certificates for electronic seals ("QSealC") and the qualified certificates for website authentication ("QWAC"), for secure communication between the respective PSPs in the provision of services under PSD2. The issues stemming from the technical nature of the eIDAS certificates have been sufficiently addressed, in particular, by EBA's

[225] Deutsche Bank, "EU Funds Transfer Regulation 2015: A regional regulation with a global impact", 2017.
[226] SEPA Credit Transfer Scheme Rulebook.
[227] European Commission, 'Digital Identity for all Europeans'. Available at: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en.
[228] See the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281. And the version amended by the European Parliament, 'Draft Report on the proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity. Available at: https://www.europarl.europa.eu/doceo/document/ITRE-PR-732707_EN.pdf.

interpretative measures. However, it is worth noting that the smooth functioning of the use of eIDAS certificates in relation to the provision of payment services, in particular in a situation where the PSP's authorisation is revoked, relies on strict adherence to the processes introduced in both the eIDAS as well as PSD2.

The objective of eIDAS is to lay down the standards across the EU required for trust service providers and the provision of trust services through technical mechanisms, such as digital certificates and cryptographic signatures. The intersection between eIDAS and PSD2 consists in the use of trust services under eIDAS in the provision of payment services under PSD2. In this context, the provision of payment services under PSD2, specifically those under Articles 65, 66, 67 and 97 foresees, *inter alia*, secure [electronic] communication between the respective PSPs, whereby the responsibilities of the particular PSPs are further elaborated in the RTS under Article 98 of PSD2,[229] or further construed in the EBA's interpretative measures.[230]

The secure communication between the respective PSPs foresees the use of eIDAS certificates under eIDAS, namely QWAC and/or QSealC in addition to a requirement on the encryption of the communication. However, there is ambiguity on the use of the particular eIDAS certificates with regards to the mutual identification within the communication, in particular regarding the ASPSP. In this regard, EBA clarified that the AISPs, PISPs and CBPIIs in order to identify themselves towards the ASPSPs may alternatively use (i) QWACs and QSealCs in parallel, (ii) QWACs only, or (iii) QSealCs with an additional element that ensures secure communication. However, no specific obligation is in this case imposed on the ASPSPs, although the EBA strongly recommends that the ASPSPs obtain and use both QWACs and QSealC in parallel for the purpose of mutual identification between the ASPSP and the AISP, PISP or CBPII; that approach was reiterated by EBA in its Q&A.[231]

There is a lack of clarity concerning the use of single or multiple eIDAS certificates. The EBA tackled the issue stating that where the PSP carries out activities referring to two or more possible PSP roles under PSD2, it is upon the PSP concerned to decide whether to use single or multiple certificates for each role. Nevertheless, where the PSP provides services through agents or EEA branches, or where it has outsourced to technical service providers some of the activities related to access to the online accounts held within the ASPSP, the EBA recommends using multiple certificates simultaneously: one per agent, EEA branch or technical service provider.

In addition, EBA has also provided clarification on the use of eIDAS certificates in respect of the possible PSPs' roles under PSD2 associated with the provision of payment services under PSD2, namely account servicing, payment initiation, account information and issuing of card-based payment instruments (and the corresponding roles of the ASPSP, AISP, PISP and CBPII). In brief, the EBA concluded that the eIDAS certificate should be limited to the payment services for which the respective PSP has been authorised. At the same, the EBA recalled its recommendation for the ASPSPs to obtain and use the eIDAS certificate (for ensuring secure communication, in particular, in respect of mutual identification between the ASPSP and AISP, PISP or CBPII).

Since the provision of payment services is a business activity that is unstable, there is an issue concerning the accuracy of the PSP's eIDAS certificate. The essence of the issue consists in the fact that the termination of providing payment services or a revocation of authorisation to provide those services, does not automatically cause invalidity of an eIDAS certificate. As a result, a situation where the PSP, that is still holding the eIDAS certificate, but

[229] 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 standards for strong customer authentication and common and secure open standards of communication (OJ L 69, 13.3.2018, p. 23-43).

[230] In particular, Opinion of the European Banking Authority on the use of eIDAS certificates under the RTS on SCA and CSC.

[231] See Q&As: 2018_4413 Qualified certificate under eIDAS for ASPSP.

lacking the respective authorisation to provide payment service, continues in the provision of those services, including in communicating with other PSP counterparts,[232] may take place. The adjacent issue refers to the possible ways of ensuring the revocation of an eIDAS certificate.[233] In order to reinforce those ways, the EBA clarified in its opinion that the competent authorities may establish a standardised process for the exchange of notifications between the competent authority and the qualified trust service provider regarding the revocation of eIDAS certificates for the purpose of PSD2.

MiCA

Concerning the interplay between MiCA and PSD2, the pieces of legislation complement each other in marginal situations, namely when the crypto asset service provider provides, *inter alia*, payment services. Further clarification on the consumer protection and safeguarding stemming from the complementarity is considered as beneficial for improving the legal certainty and setting a level playing field.

From a broader perspective, the issue of the possibility of merging PSD2, EMD2 and MiCA may also be considered. Like EMD2, MiCA complements the wider area of financial services that may considered as being payment services (or services closely associated with the payment services under PSD2). However, the main issue to be resolved is whether it would be possible to replace three legal measures (thus establishing a broader legal instrument governing the field of payment and closely related services) by a single measure or whether the existing MiCA could only partially be incorporated into the merged legal instrument.

The objective of MiCA is to establish a legal framework for hitherto unregulated crypto-assets. The complementarity between MiCA and PSD2 refers to a situation in which the crypto asset service provider ("CASP") provides payment services as part of its crypto asset services.[234] In such a case, the CASP is to be authorised under PSD2 or appoint the PSP that is authorised under PSD2.

Against this background, with regards to the interplay of PSD and MiCA, clarification would be desirable in respect of the CASP contracting with a payee to accept crypto-assets other than e-money tokens, in particular, whether such CASP would need to meet the same requirements on consumer, security and operational resilience as the regulated PSP. Currently, MiCA lays down less consumer protections in comparison to PSD2 (that apply for payments made with e-money tokens, or other types of funds under PSD2).[235] In this context,

---

[232] For the sake of completeness, in such a scenario, apart from an infringement of PSD2, continuing to provide payment services would also have other consequences, for instance, an infringement of GDPR etc.

[233] In this context, the qualified trust service providers are responsible for checking the validity of the information in the eIDAS certificates at the time of issuance, and both the qualified trust service providers and PSPs are responsible for ensuring the information is kept up to date and for revoking the certificates.

[234] According to ECB's Opinion of the European Central Bank of 19 February 2021 on a proposal for a regulation on Markets in Crypto-assets, and amending Directive (p. 5) "Asset-referenced and e-money token arrangements may qualify as tantamount to that of a 'payment system' where they have all the typical elements of a payment system:

(a) a formal arrangement;

(b) at least three direct participants (not counting possible settlement banks, central counterparties, clearing houses or indirect participants);

(c) processes and procedures, under the system rules, common for all categories of participants;

(d) the execution of transfer orders takes place within the system and includes initiating settlement and/or discharging an obligation (e.g. netting) and the execution of transfer orders, therefore, has a legal effect on the participants' obligations; and

(e) transfer orders are executed between the participants" and (p. 6)

"Similarly, the function of asset-referenced and e-money token arrangements that set standardised and common rules for the execution of payment transactions between end users could qualify as a 'payment scheme'".

[235] The consumer protection under PSD2 includes, *inter alia*, protection in case of lost payments, incorrect payments, limits on liability for fraudulent transactions, consumer focused dispute resolution etc.

the first step should be to determine whether those activities can be identified as the 'acquiring of payment transactions' within the meaning of PSD2.

Further clarification is also recommended with regards to the treatment of safeguarded funds under MiCA and PSD2. According to Article 44(7) of MiCA, MiCA stipulates direct access to safeguarded funds, in case the offeror of an e-money token does not redeem within 30 days, to the holder of e-money token. Thus, in that case, the level of protection under MiCA goes beyond PSD2. Possible confusion of rules to be applied may arise in a situation where funds are safeguarded using the insurance method.

AI Act

Making use of AI, including biometrics, in the provision of payment services under PSD2 may bring benefits, in particular, in strengthening authentications and supporting fraud detection.

The effort of PSD2 is to be technologically neutral to adequately respond to ICT developments. In practice, making use of AI in the provision of the payment services under PSD2 has to be in line with other legal measures associated with AI, including the legal instruments governing, for instance, ICT security, including cyber-security, the provision of services by third-party providers, the personal data protection, etc. As mentioned above, due to its technological neutrality, no legislative action is needed within the PSD2 revision in respect of the AI Act.

Data governance act, Data act

The issue of data as part of the data governance and data acts relate to PSD2 rather indirectly. These acts govern the subsequent use of data produced within or in connection with the provision of payment services under PSD2.

The data governance act, data act and the open data directive are part of the European strategy for data that aims to create a Single Market for data.[236] The data governance act governs the processes and structures to facilitate data-sharing by companies, individuals and the public sector, while the data act clarifies who can create value from data and under which conditions.[237]

As already mentioned above, one of PSD2's characteristics is its technological neutrality, thus, no legal action within the PSD2 revision is needed (for instance, due to the rapid technological progress in IT, it would not be desirable to incorporate provisions on API within the revised PSD2 etc.). However, like with the AI Act, compliance with other legislative measures (covering *inter alia* cyber-security, personal data protection etc.) must be ensured within the re-use of data originally processed in the provision of payment services under [revised] PSD2.

5.4.3. How will PSD2 rules on operational and security risks. interact with the rules of the Commission´s regulation on digital operational resilience for the financial sector (DORA)?

Concerning operational and security risks, the scope of PSD2 and DORA partly overlap. The main difference consists in the fact that PSD2 framework for operational and security risks addresses both ICT as well as non-ICT risks, whereas DORA focuses specifically on ICT risks.

The new digital operational resilience framework (set out by DORA Regulation and accompanying DORA Directive) is set to enter into force in 2023 and to apply as of 2025. This new framework will apply to certain entities in the scope of PSD2: credit institutions, payment institutions (including payment institutions which have been exempted pursuant to accordance Article 32 (1) of PSD2), account information service providers referred to in Article 33(1) of

[236] European Commission, "A European Strategy for data"
[237] European Commission, " Data Act – Questions and Answers".

PSD2 and electronic money institutions, including electronic money institutions exempted pursuant to Article 9 (1) of Directive 2009/110/EC.

The new rules on digital operational resilience for those entities will consequently be those which are set out by DORA (i.e., rules on ICT risk management, incident reporting, testing, ICT third-party risk management, information sharing on cyber threats). In respect to Article 95 PSD2 (management of operational and security risks) PSD2 applies comprehensively (i.e. to all types of security risk) but those PS rules will be in future without prejudice to the full application of ICT risk management requirements laid out in Chapter II DORA (which would apply instead).

Moreover, with a view to avoiding the complications and burdens of dual reporting regimes, all operational or security payment-related incidents – previously reported pursuant to PSD2 – would be in future reported under DORA and irrespective of whether such incidents are ICT-related or not.

To achieve consistency between new rules and current guidelines, the relevant ESA guidelines would need to be updated in the future to ensure their coherence with the new digital operational resilience framework (DORA).

5.4.4. With regards to data protection, how do PSD2 provisions on access to payment accounts and the processing of personal data for payment purposes adhere to the GDPR and EDPB Guidelines? In particular, is there a need to further align and ensure complementarity and consistency between PSD2 and GDPR? In that respect, is there a need for a clarification regarding the basis for the processing of personal data for payment purposes?

In the provision of payment services under PSD2 the processing of personal data takes place, subject to GDPR (and EUDPR), as an EU regulation with direct effect,[238]. GDPR, respectively EUDPR, apply alongside with PSD2; whereas PSD2 does not represent *lex specialis* to GDPR/EUDPR.[239] In this context, due to its general nature, GDPR is applicable regardless of being expressly mentioned in Article 94 PSD2.

The interplay of PSD2 and GDPR, including the topic of appropriate legal grounds for the processing of personal data for the purposes under PSD2, is addressed in European Data Protection Board (EDPB) interpretative measures, in particular, EDPB Guidelines 06/2020.

In general, GDPR[240] lays down a strong and coherent personal data protection framework, that is to be applied in a consistent way throughout the Union. Further, the European Central Bank may act as the PSP, thus compliance with EUDPR[241] is applicable, too; in addition, the European Supervisory Authorities, in particular the European Banking Authority, should guarantee fair competition in the market under PSD2, whereby processing of personal data may occur in that context, too. The interplay between GDPR, respectively EUDPR, and PSD2 is explicitly mentioned in Article 94 of PSD2, complemented by a further explanation in Recital 89 of PSD2. As a general conclusion, both PSD2 provision and recital concerning personal data protection note the aforementioned compliance with the Union data protection framework.

[238] See Article 288 of the TFEU.

[239] European Data Protection Board, "Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR", 2020. Bird & Bird, "EU: The interplay of PSD2 and GDPR – some selected issues", 2019.

[240] 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) (OJ L 119, 4.5.2016, p. 1-88).

[241] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39-98).

The topic of granting access to payment accounts is governed by Article 66 and 67 of PSD2. More specifically, according to Article 66(1) and 67(1) of PSD2, the obligation guaranteeing the payment service user to make use of services enabling access to account is imposed on the Member States, meaning that Member States are responsible for adopting national legislation granting access to payment accounts. From the personal data protection perspective, the topic has been addressed by the EDPB in its Guidelines 06/2020.[242] The EDPB held that the processing of personal data by the ASPSP consisting of granting access to the personal data requested by the PISP and AISP in order to perform their payment service to the payment service user is based on a legal obligation. Thus, the applicable legal ground for processing personal data in this case is Article 6(1)(c) of GDPR, that is to say, that the processing is necessary for compliance with a legal obligation to which the controller is subject. According to the EDPB, the obligation to grant access to payment accounts should stem from national law transposing PSD2.

Although there are no doubts about the legal ground for the processing of personal data at stake, it is worth thinking about consequences of that conclusion in practice. As PSD2 is a directive to be transposed, national law regularly jeopardises the homogenous application of Union law through 'gold-plating'. However, a guidance elaborating on the notion of the legal ground under Article 6(1)(c) of GDPR is provided for in Opinion 06/2014.[243] For Article 6(1)(c) of GDPR to apply, the legal obligation must be imposed by law, but it is permissible that the legislation set only a general objective, while more specific obligations are imposed at a different level, for instance, either in secondary legislation or by a binding decision of a public authority in a concrete case. With regard to EBA's role mentioned in Recital 33 of PSD2 it may be worth considering making use of EBA's measures to specify the obligations relating to the processing of personal data in the context of granting access to payment accounts; nevertheless, it should be reiterated that such a measure would need to be a binding one. To conclude, the provisions of PSD2 concerning access to payment accounts are consistent with GDPR, providing a sufficiently clear basis in respect of a legal ground for personal data processing to be applied. The risk of heterogeneous application of PSD2 (in particular, the accompanying risk of forum shopping) stems from national law transposing the PSD2. That risk may be mitigated by laying down the details on personal data processing in the context of granting access to payment accounts in an EBA measure that is of binding nature.

From a broader perspective, extending the topic of determining an appropriate legal ground for processing of personal data under PSD2, no specific action is needed within a review of PSD2. PSD2 assumes processing of personal data in various situations, whereby an adequate legal ground may, depending on a particular processing activity, vary accordingly. The prevailing part of personal data processing is underpinned by the legal ground concerning the performance of a contract for the use and/or provision of payment services. Nevertheless, the data controller should be precautious in applying that legal ground, as this legal ground may be applied on condition of a necessity and other requirements;[244] clarification on the use of this legal ground is provided in WP29's or EDPB's guidelines, or opinions respectively.[245]

As mentioned above, compliance with legal obligation may be used as the legal ground (for instance, in the context of granting access to the personal data requested by the PISP and AISP in order to perform their payment service to the payment service user). Further, the legal

[242] See Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR, p. 12.

[243] See Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, p. 19-20.

[244] For more details, see Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, p. 9-12.

[245] For instance, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.

ground consisting in the legitimate interest of the controller or a third party may be applied in some cases, too.[246]

Interpretation issues occurred in respect of the notion of 'consent' or 'explicit consent'. A consent is one of the legal grounds listed in Article 6(1) of GDPR,[247] whereas PSD2 uses that notion on many occasions,[248] but in a different meaning than that in GDPR. In essence, one notion, i.e. 'consent', is used by two branches of law (financial law, including payment services law and personal data protection law). The possible inconsistency between PSD2 and GDPR has been overcome in Guidelines 06/2020, concluding that the notion of consent used in PSD2 is a contractual [consent] in nature. As a result, the word 'consent' in PSD2 has the meaning 'entering into contract/concluding a contract'. To the contrary, it is not used within the meaning under GDPR as being a legal basis allowing for the processing of personal data associated with a contract under PSD2; the proper legal basis for that processing is the legal basis 'provision of a contract' under Article 6(1)(b) of the GDPR. However, the fact that the processing of personal data connected with a contract under PSD2 does not rely on consent as a legal basis does not mean that the consent as a legal ground under GDPR cannot be (on other occasions presuming processing of personal data) used as a legal ground for processing of personal data under PSD2.[249] To sum up, PSD2 and GDPR are consistent in terms of legal grounds to be applied in respect of personal data processing under PSD2; determining an adequate appropriate legal ground for a particular processing under PSD2 is upon the PSP [the controller], whereby in doing so, the PSP is equipped with guidance measures developed by the EDPB (or its predecessor, the WP29).

Apart from the topics mentioned above, it is worth noting that the EDPB Guidelines 06/2020 have also solved various alleged inconsistencies between GDPR and PSD2, raised by market participants or other stakeholders over time, concerning, for instance, processing of special categories of data, processing of silent party data, application of the principle of data minimisation etc.;[250] thus, no legislative action withing the PSD2 review is needed in respect of those issues. Since in practice the market participants mostly struggle with the processing of special categories of data and the principle of data minimisation, both topics are elaborated further.

The processing of special categories of data within the provision of services under PSD2 refers, in particular, to the processing of biometric data. For the processing of special categories of personal data a 'general' legal basis under Article 6(1) of GDPR (described above) and a 'special' legal basis (or more precisely an exception to the general prohibition of processing of special categories of personal data) under Article 9(2) of GDPR. The 'legitimate interest' under Article 6(1)(f) GDPR may be used as the 'general' legal basis. Further, considering a suitable condition for processing under Article 9(2) of GDPR, the EDPB Guidelines 06/2020 identify substantial public interest [on the basis of EU or Member State law] under Article 9(2)(g) of GDPR as such a suitable condition; and where such substantial public interest [on the basis of EU or Member State law] making use of the explicit consent is limited in practice, as the explicit consent must meet all criteria of a consent under GDPR (enumerated in Article 4(11) and 7 thereof). One of the criteria is that consent is freely given. This may be challenging in practice, as the provider of services under PSD2 would need to implement, for instance within the processing of biometrics for authentication, a system

[246] For instance, processing of silent party data when that processing is necessary for purposes of the legitimate interests pursued by a controller or by a third party.

[247] For more details, see Guidelines 05/2020 on consent under Regulation 2016/679.

[248] For instance, in Article 4(23), Article 52(2)(c), Article 64 etc.

[249] Consent as a legal ground may be relied on, for instance, in case of personal data processing for a purpose other than that for which the personal data have been collected. The processing for 'other purpose' refers to some processing activities carried out by AISP or PISP.

[250] See, for instance, the comments on the interplay of GDPR and PSD2 provided by the European Payment Service Providers, Bird & Bird etc.

processing biometrics (for those users consenting) and a parallel system that does not process biometrics (for users not consenting). Therefore, the reliance on the substantial public interest [on the basis of EU or Member State law] under Article 9(2)(g) of GDPR is a more suitable 'special' legal ground for the processing of special categories of personal data in the provision of services under PSD2. Although Article 9(2)(g) of GDPR provides for requirements in respect of EU (or Member State) law introducing the substantial public interest, GDPR (Article 9(2)(g), recital 52) is silent regarding further elaboration on the notion of the 'substantial public interest'.[251] Clarification on this notion was provided, for instance, in the UK statutory instrument which states that processing of special categories of personal data in the substantial public interest relates to the processing for the purposes of the prevention or detection of any unlawful act, or to discharge functions which protect members of the public from certain conduct which may not constitute an unlawful act, such as incompetence or mismanagement. The nature of processing of biometrics for the purposes of authentication meets the aforesaid clarification on the substantial public interest. In respect of the PSD2, the revision should focus rather on checking whether the current wording meets the general conditions of Article 9(2)(g) of GDPR, than explicitly stating that the processing of biometrics is possible under revised PSD2; the possibility to rely on Article 9(2)(g) of GDPR stem from compliance with the general conditions enumerated therein, but not in mere, though explicit, wording referring to biometrics in the revised PSD2.

Concerning data minimisation, the principle of data minimisation is laid down in Article 5(1)(c) of GDPR providing that the processing of personal data is to be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". The EDPB in Guidelines 06/2020 further clarifies on this topic that the controllers should process no more personal data than what is necessary in order to achieve the specific purpose in question; meaning in the context of the provision of services under PSD2 that the amount and the kind of personal data necessary to provide the payment service is determined by the objective and mutually understood contractual purpose.[252] The amount and kind of data to be processed is based on a particular service, and they may vary over time (for instance, due to technological developments or amendments to the legislation). Therefore, it is not desirable to provide, in particular, exhaustive lists of personal data to be processed within the provision of services under the revised PSD2; nor is it desirable to provide opened lists of personal data to be processed (as those would be mere superfluous wording). Thus, there is no action needed in respect of the revised PSD2 in relation to the data minimisation principle.

However, from a broader perspective of coherence and consistency of PSD2 and GDPR in the context of processing personal data for payment purposes, of particular attention is Article 33 PSD2. According to Article 33(2) of PSD2, the AISP is to be treated as the payment institution, whereby, *inter alia*, Title IV of PSD2, save for some exceptions, does not apply to the AISP. Title IV of PSD2 covers, *inter alia*, Article 94 governing personal data protection, while this provision is not covered in the list of the said exceptions. However, the AISP within providing the services under point (8) of Annex I of PSD2 processes personal data.[253] The existing wording of Article 33(2) of PSD2 may cause misinterpretation regarding compliance with the personal data framework (i.e. although exempted under PSD2, the AISP still need to comply with GDPR due to its general applicability). As a result, legislative action to extend the list of exceptions in Article 33(2) of PSD2 would be desirable. To that end, the respective wording of Article 33(2) of PSD2 should be adjusted, in the simplest way, by replacing figure '95' with figure '94'.

---

[251] Data Protection (Processing of Sensitive Personal Data) Order 2000.

[252] See Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR, p. 21.

[253] For instance, the AISP, while providing its services, falls within the definition of 'obliged entity' under Directive (EU) 2015/849, which compels the obliged entity to perform due diligence with regard to a customer, whereby that action inevitably requires personal data to be processed.

5.4.5. *Is there a need to incorporate rules laid down in Delegated Acts and further EBA guidance into a possible revision of PSD2 and vice versa? If so, which one(s) and at which level? If not, why?*

EBA GLs on authorisation of payment and electronic money institutions should be elaborated into a more practical way, expanded and ultimately converted into a RTS as has been already presumed and outlined under Article 5(6) of PSD2. Some of the Member States (CZ) have already transposed necessary elements from the GLs on authorisation in the upcoming amendment to its secondary legislation (two Decrees of the Czech National Bank, effective as of 1 July 2022), which are legally binding, as opposed to the soft-law GLs, where a 'comply or explain' mechanism applies.

Over time, EBA has developed a profound structure of measures addressing market participants' queries on alleged inconsistencies concerning the pieces of legislation in relation to which the EBA exercises its oversight powers. This also applies in respect of issues under PSD2. In this regard, the EBA based on quantitative assessment (the number of market participants queries on a particular issue under PSD2) as well as qualitative assessment (profoundness of a query, author of a query, e.g., whether an interpretation is sought by a professional association or a 'simple' market participant) is best placed to identify PSD2 topics to be clarified in an opinion or Q&As (including topics extending strictly PSD2, for instance, the interplay among PSD2, FTR and AMLD). OBJ.

Since the above said EBA's framework is on one hand robust and on the other hand sufficiently granular, only marginal incentives for adjustments may be provided. For the sake of improving the effectiveness of market participants in complying with the respective requirements under PSD2, some main concepts may be further elaborated. Apart from the concepts already mentioned above, a possible action may cover embedding the SCA elements, currently detailed in the dedicated opinion[254] in a RTS. In this regard, for instance, a simplified set of criteria on the particular elements (i.e. inherence, possession and knowledge elements) in a RTS may provide stronger legal clarity and consistency in the use of SCA, provided that such an adjustment maintains technological neutrality and keeps the ability to address further progress in the field of ICT tools enabling the SCA.[255]

The EBA may also focus on the threshold under Article 32(1)(a) of PSD2. In this regard, EBA guidelines providing a methodology for calculating the threshold may reinforce the fulfilment of the respective obligations under PSD2 by market participants. The guidelines may *inter alia* address the types of transactions to be included in or excluded from the calculation of the threshold, provide examples of underlying values to be used for the calculation with regard to the particular payment services, etc.

Further in this context, the EBA may consider developing guidelines elaborating and aligning the definitions under both PSD2 as well as EMD2 (in order to prevent from forum shopping stemming from uneven interpretation of the definitions within the national transpositions and subsequent practice); the same is applicable in respect of the scope and exemptions under PSD2. Guidelines providing for an overview of reporting obligations in a clear and structured manner would facilitate the fulfilment of obligations in this field.

Finally, as a general remark and recommendation on the way of addressing the need to either incorporate rules in Delegated Acts or developing further EBA guidance, it may be advised to keep the payment services framework as flexible as possible, unless there is a need for a common understanding of a particular issue; in other words, the objective, including the understanding of the crucial concepts and setting, is compulsory, but ways to reach the objective are kept flexible.

[254] Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2.

[255] Perspectively??,, a shift from the Open Banking to the Open Finance.

5.5. EU added value

This section analyses the extent to which the PSD2 has produced results beyond what would have been achieved by Member States acting alone. The ultimate aim is to understand whether EU intervention was justified when the PSD2 was adopted and whether it continues to be justified today.

As a result the findings in this section are very closely related to the previous sections on relevance, effectiveness, efficiency and coherence which have analysed the impact of the PSD2 at EU and Member State level. To avoid duplication, this chapter refers to the findings of previous sections where they help understand EU added value, without however repeating the full analysis. Like the other chapters of this review, it is based on desk research, stakeholder questionnaires and expert input and it is subject to the same limitations as the rest of study, namely the fact that not all the benefits of the PSD2 have materialised yet the available data is not always comparable across countries and stakeholder groups. Furthermore, it is difficult to estimate the development of the market without the PSD2, as the entire market is currently undergoing a strong transformation. While this transformation has partly also been triggered by PSD2, some of the developments precede the PSD2 and some of them are driven by technology developments and other factors and they cannot be fully attributed to regulatory changes such as the PSD2.

With these caveats in mind, the analysis of EU added value touches on the following evaluation questions:

- Specific to EU added value:
- Has intervention at EU level been justified, and does it continue to be justified?

Related to effectiveness:

- To what extent did PSD2 improve the functioning of the internal market?
- Did PSD2 help in establishing and fostering an EU-wide level playing field (e.g., information symmetries, same interests and closing regulatory gaps) in payment services?
- Are there any barriers for banks, new entrants (FinTechs), or third-party providers in providing data sharing services based on PSD2 rules?
- Do PSD2 rules on SCA effectively ensure a competitive level playing field among all payment service providers and do they ensure a technology and business-model neutrality?
- Has the licensing regime contributed to a level playing field between the various actors, especially with regards to new actors (e.g., payment initiation services providers and account information services providers) that are subject to the licensing requirements?

Related to coherence:

- How has the interaction between PSD2 licensing regime with EMD2 been? Is there need for further alignment between the two to ensure a level playing field?
- Are there gaps or diverging approaches in the way Member States are applying PSD2 that prevent PSD2 from achieving its objectives? If any, are amendments necessary to narrow the scope of application?
- How far do regulatory practices (e.g., regarding enforcement of PSD2 rules) diverge across Member States? Do they need further harmonisation? Should any part or all of PSD2 be transformed into a Regulation, taking into account a cost-benefit analysis?
- Are (additional) actions at EU level needed or justifiable to ensure a (further) coherent and effective supervision of payment services (i.e., to ensure a harmonised supervisory approach in the field of retail payments activity and with other EU financial legislation)? Is there a need to introduce specific or additional supervisory powers at EU level? How could these supervisory powers be designed?

5.5.1. Internal market, competition and innovation

The study (Section 5.2) finds that the PSD2 has been a major step forward for the development of payments markets in Europe:

- PSD2 has allowed for greater competition as new businesses, new business models have entered the market which have fostered innovation and provide more choice for consumers in the way they pay online.
- PSD2 provided the legislative and regulatory foundations for Open Banking and it has improved the general level of the security of payment transactions through the implementation of Strong Customer Authentication.
- The impact of PSD2 has been particularly marked in markets which were under-developed in terms of innovative drive and FinTech solutions.
- From an EU perspective, PSD2 provides a foundation and a common set of (albeit imperfect) rules across the EU facilitating the adoption of electronic means in the EU.
- PSD2 has contributed to a certain extent to developing cross-border payments within the EU (through the passporting procedure) and enhancing the quality of such payments.

At the same time, Chapters 3 and 5.2 have shown that, despite the PSD2, the payments market is still domestically oriented in most countries.

- While the PSD2 has made cross-border operations in payments market easier, Chapter 3 and 5.2 show that credit transfer or cards of domestic payment solutions remain fragmented on national borders. There is a lack of interoperability in existing national schemes, infrastructure and solutions.
- Transposition and implementation delays have meant that fragmentation along national borders persists.
- Some stakeholders have questioned whether the economic benefits that PSD2 has undoubtedly brought are commensurate with the costs, especially in the earlier stages of implementation where benefits have not yet fully materialised.

5.5.2. Creation of a level playing field across the EU, regulatory gaps and divergence

The PSD2 has contributed to establishing a level playing field across the EU and aligning national rules when it comes to payment markets but significant room for improvement remains in fostering legal certainty for all market participants, reducing regulatory divergence across countries and ensuring greater coherence between the PSD2 and other legislation.

- The PSD2 has increased the level of legal certainty for new payment service providers, by structuring the legal environment for payment services.
- The PSD2 and the EMD2 are strongly related and generally coherent with one another to the point there is significant support for the two Directives to be merged to reduce the risk of the legal framework becoming out of date. At the very least, there is a need for clarification of the definition of the two services to prevent regulatory arbitrage.
- Where there are differences between Member States, these can be partially linked to underlying market conditions (e.g., the level of digital maturity) which varies across the EU.
- PSD2 has improved the security of payment transactions through the implementation of Strong Customer Authentication (SCA) which represents a true EU added value.
- Overall, the current licensing requirements strike the right balance between, financial stability, consumer protection and with the accelerating market take-up of open banking and the innovative development of open banking solutions.
- Most consulted stakeholders (market players and authorities) consider the supervision of PSPs at EU and Member State level to be improving as a result of PSD2.

At the same time, the functioning of the internal market continues to be affected by a lack of harmonisation in national rules, and lack of clarity when it comes to coherence with other legislation.

- Margins of discretion in transposing and implementing PSD2 across Member States have led to asymmetries and national specificities (e.g., in applying exemptions) which hamper cross-border competition.
- Uneven application of the PSD2 can be attributed to unclear definitions of basic concepts underlying the Directive (e.g., the notion of "payment account") and divergent interpretations of obligations among Member States.
- The interpretation of the level 2 text also contributes to divergence in rules (e.g. passporting) and regulatory arbitrage, with payment firms choosing jurisdictions where they allegedly obtain an 'easier' authorisation.
- Barriers to a level playing field derive not only from the wording of the Directive but also from reporting requirements requested by local authorities which differ widely across countries.
- Collaboration between supervisory bodies and with EBA is insufficient to provide clear guidance (e.g., on how Member States define an acceptable API).
- There remains an unlevel playing field between banks and TPPs. TPPs tend to be small companies and their competitive advantage comes from their ability to move fast. The slow pace of implementing APIs has clearly benefited banks, while TPPs had their costs increased to satisfy the new regulatory obligations.
- The implementation of PSD2 required high levels of investment, which resulted in opportunity costs as developers could not work on new products.
- Methods for access to accounts remain fragmented across the EU and continue to be a significant challenge for PISP/AISP to adapt processes to each ASPSP. In particular, PISPs stated that a lack of clarity in the Directive enabled banks to interpret the level of accessing account information by limiting the data that PISPs can access.
- While PSD2 created a structured legal environment for payment services, allowing them the possibility to passport their licence and provide services across borders, different national authorities place different regulatory requirements on PSPs operating across borders which has made such activities difficult.
- When it comes to SCA, the complexity of the rules and differences in implementation timeframes across Member States have led to a (temporary) unlevel playing field and to legal uncertainty as SCA is not implemented uniformly across the EU.
- Differences in licensing regimes (e.g., on CDD and KYC) between countries remain and licensing rules should be clarified to minimise divergence and the consequent forum-shopping among licencees.

Overall, drawing on the results of the evaluation presented in other sections of the report, this chapter shows that the PSD2 was and continues to be justified as it has brought considerable EU added value. This is further corroborated by the fact that the majority of interviewed stakeholders consulted for this study welcomed the intervention and none of the market players consulted for the study were in favour abolishing the PSD2. However, this does not mean that there is no room for improvement and the section has highlighted a range of areas where further EU value added could be created. Some of these areas are further discussed in the next chapter which summarises the results of the evaluation and provides recommendations.

6. Conclusions

This chapter presents overarching conclusions of the review followed by a set of general and specific recommendations based on those findings. The conclusions represent a summary of the key findings of the review for each evaluation dimension. More detailed findings and conclusions can be found in the main text of Chapter 5.

6.1. Key conclusions of the review

Relevance

Relevance of PSD2 in light of market developments and policy priorities

The needs present at the inception of PSD2 largely continue to be relevant today. The only exception is the need to harmonise charging practices across Member States which has largely been achieved as a result of the surcharging ban. Indeed, the surcharging ban has harmonised charging and steering practices for a large share of payments in the EU. Where divergences exist, and a surcharge can still be charged, this concerns only a fraction total payments. Also, in the rare case that they are charged, surcharges can no longer surpass the actual costs the merchant incurs for accepting the payment.

Continuing market developments, i.e. market developments that were present at the inception of PSD2 and continue to this day, affirm the relevance of a number of needs underpinning PSD2. For example, the need for more effective competition remains relevant in light of (continued) limited market penetration of innovative payment solutions and fragmentation of the European payments market. Other examples include the need for more harmonisation of licensing and supervisory practices and increased consumer protection. Divergences in supervisory practices as well as developments in consumer fraud affirm the relevance of these needs.

New market developments similarly affirm the relevance of some of the needs that PSD2 aims to address. For example, the needs to regulate the status of all payment service providers and for more effective competition. These needs remain relevant as a result of the emergence of premium APIs and API aggregators. Other needs that new market developments affect are the needs for less fragmentation of the European payment market and a more autonomous and resilient European payments market. The growth of domestic account-to-account payment schemes affects the first, whereas the entry of BigTechs to the European payments market affects the latter.

Finally, future policy developments have the potential to affect the needs surrounding the competition within, fragmentation of, and autonomy and resilience of the European payment market. Most potential lies in the development of a pan-European payment solution and the adoption of instant payments. Were they to materialise successfully, they would reduce the needs for more competition, less fragmentation and more autonomy and resilience in and of the European payments market.

Expected future evolution of needs

Future developments in the payments market may impact the needs underpinning PSD2. For example, the introduction of a digital euro, or the uptake of crypto-assets as a common form of payment, may increase competition and decrease fragmentation in and of the European payments market.

Other needs, such as for increased consumer protection or for a more autonomous and resilient European payments market, may similarly be affected. The uptake of crypto-assets as a payment method may affirm the relevance of increased consumer protection as they are complex assets to understand. The adoption of a digital euro, i.e. a homegrown payment

solution, would make the European payments market more autonomous and resilient (and thus reduce the relevance of that need).

Extent to which PSD2 addresses current developments in the field of payment services

The objectives of PSD2 continue to a large extent to address the current needs. The exception is the objective on steering charging practices across countries which has become less relevant as it has to a large extent been achieved. Also, when a new need to strengthen the autonomy and resilience of the European payments market is introduced, accompanying objectives will have to be formulated.

Effectiveness

Overall, there has been progress in meeting the goals of the PSD2 though issues in implementation have meant these goals have not been fully met and market actors have faced some difficulties in operating in the new legislative environment.

Compared to previous legislation, the PSD2 has been a major step forward for the payments industry and it has brought about important benefits. For instance, it has allowed for greater competition and innovation as new businesses and business models have entered the market.

Moreover, PSD2 provided the legislative and regulatory foundations for Open Banking, it has improved the security of payment transactions through the implementation of strong customer authentication (SCA) and it has facilitated the adoption of electronic means of payments in the EU.

SCA has been successful in establishing a high level of protection for payment service users and fraud levels have dropped, but this has come at a significant cost. At the same time, the PSD2 has also increased consumer rights in various areas such as reduced liability for unauthorised payments and unconditional refund rights for direct debits in euro.

On the other hand, the study finds that the SCA requirement has made the customer journey in a transaction more difficult which can mean that consumers do not complete e-commerce transactions.There remain loopholes in SCA which allow for fraudsters to circumvent security provisions

PSD2 has contributed to a certain extent to developing cross-border payments within the EU and enhancing the quality of such payments but the EU market remains fragmented along national lines and consumer awareness remains low. This is problematic because the share of fraudulent transactions is significantly higher for cross-border transactions than for domestic transactions.

When it comes to open banking, the PSD2 has allowed for structured interaction between ASPSPs and TPPs but ASPSPs are concerned about the costs they incur due to the free access they are required to provide and TPPs argue that access is consistently hindered.

The vast majority of consulted stakeholders thought that the implementation of the Directive was a cumbersome and lengthy process. The biggest obstacle for banks was regulatory uncertainty, while TPPs reported issues regarding long licensing procedures and cross-border payment initiations due to technical challenges. Several provisions within the PSD2 have not been implemented in a harmonised way across Member States which has created difficulties for entities seeking to provide services across borders.

When it comes to supervision, there is agreement that supervision has increased as a result of the Directive but supervisors have not been able to address key issues raised by both TPPs and ASPSPs effectively and efficiently, which in turn has hampered their ability to provide services in line with the expectations of PSD2.

Finally, the consulted stakeholders agreed that the intention behind the PSD2 is appropriate but that they have led to disproportionate requirements on PSPs when it comes to transparency requirements, licensing regimes, and SCA.

Efficiency

The costs associated with the implementation of PSD2 are significant and the largest cost items are:

- Open banking, in particular API-development (estimated at EUR 3.2bn)
- SCA rollout, notably implementation costs (estimated at ~ EUR 5bn) and an increase in transaction failure rates (estimated at up to EUR 33.5bn)
- Legal interpretation and uncertainty

The main benefits linked to PSD2 are:

- Improvement of the functioning of the Single Market (including increased market access for TPPs in the order of EUR 1.6bn),
- Unlocking the potential for innovation, especially when it comes to modernisation of IT infrastructure, open banking and the further development of consumer services (like financial planning tools),
- More secure payment environment for customers and a reduction in fraud rates (worth ~ EUR 0.9bn per year), especially for more tech savvy consumers

The overwhelming majority of banks and associations consulted for the study suggested that the costs of the PSD2 largely outweigh the benefits to them. National authorities and TPPs established before PSD2 was introduced were more positive about the general impact but they tended to agree with the overall negative assessment.

At the same time, while the costs of the PSD2 were incurred in the initial stages (i.e. substantial investment costs), the benefits – though significant – are only materialising gradually, and it is therefore difficult to come to an overall conclusion regarding costs and benefits at this time. This is true both for market participants and for authorities where the benefits seemed to be more visible in countries with less developed payments markets.

Opportunities for simplification and maximisation of benefits

Opportunities to simplify the level 1 legislation generally relate to the reduction of legal ambiguity, the large room left for interpretation by NCAs leading to inconsistent application and improvement of the interplay of PSD2 with other legislation (e.g., GDPR, AMLD and EMD2). In addition, stakeholders would be in favour of a more technology-neutral legislation, a comment generally made for both APIs and SCA, which in their view would reduce burden. Specific aspects related to level two, namely the ’90-day rule’ and technology neutrality were also identified.

At the same time, the results of the analysis of costs and benefits suggest that the most substantial items are sunk (one-off) costs that have already been incurred. Therefore, the potential for simplification is overall relatively modest and with benefits only now becoming visible, it is too early for a comprehensive list of opportunities to maximise these benefits at this point.

Coherence

Overall, the PSD2 shows a fair degree of internal coherence but there is some evidence of incoherence when it comes to implementation stage in Member States. Specifically, Article 2 (Scope), Article 3 (Exclusions) and Article 4 (Definitions) have been the object of clarifications by EBA following questions by market participants. Ambiguity in terms of PSD2’s fundamental concepts and exemptions and the subsequent heterogenous interpretation across the Member States bring about an uneven playing field and they create an incentive for forum shopping.

Moreover, in the face of technological and market change, maintaining coherence with the overarching objective to facilitate the emergence of a well-functioning payment services market may require changes to the applicability of the PSD2 (e.g., to technical services providers).

The potential merger of PSD2 and EMD2 legal framework is a challenging but welcomed opportunity to reduce overall complexity that would bring more clarity to EU payment legislation. The interplay between the requirements on access to payment systems under PSD2 and the SFD should be addressed directly within the SFD review. In ensuring the coherence between the PSD and AMLD, it is considered crucial to follow and build upon the work conducted by EBA.

Concerning operational and security risks, the scope of PSD2 and DORA partly overlap. Article 95 PSD2 (management of operational and security risks) will in future be without prejudice to the full application of ICT risk management requirements laid out in Chapter II DORA. All operational or security payment-related incidents – previously reported pursuant to PSD2 – would be in future reported under DORA, irrespective of whether such incidents are ICT-related or not. To achieve consistency between new rules and current guidelines, the relevant ESA guidelines would need to be updated in the future to ensure their coherence with the new digital operational resilience framework.

Finally, with regards to the interplay between PSD and MiCA, clarification would be desirable in respect of the CASP (crypto-asset service provider) contracting with a payee to accept crypto-assets other than e-money tokens. In particular, it is asked whether such CASP would need to meet the same requirements on consumer, security and operational resilience as a regulated PSPN. Also, further clarification is recommended with regards to the treatment of safeguarded funds under MiCA and PSD2, as well as the definition of “funds” under PSD2.

EU added value

Overall, the PSD2 was and continues to be justified as it has been a major step forward for the development of payments markets in Europe, it has increased legal certainty and the security of payment transactions, strengthened supervision and it has brought considerable EU added value in terms of establishing a level playing field across the EU and aligning national rules when it comes to payment markets

At the same time, the evaluation shows that there is room to improve relevance, effectiveness, efficiency and coherence by further aligning rules across countries and reducing incentives for regulatory arbitrage, clarifying obligations and limiting margins for interpretation at national level, reducing implementation delays, fostering collaboration between supervisory authorities and ensuring that costs for market participants remain proportionate to the benefits.

6.2. Recommendations

This section presents a set of recommendations, based on the conclusions of the review of the PSD2. The recommendations are organised along three main pillars of improvement:

- Scope and exclusions
- Open banking, and
- Consumer protection

Recommendations on Scope and Exclusions

Improve the consistent application of PSD2 across Member States and better align licensing and supervisory rules. The study has shown that one of the main obstacles to the PSD2 fulfilling its objectives relates to the way in which it is applied in the Member States. Different interpretations of the rules and delays in implementation lead to regulatory fragmentation across the Single Market, which creates the risk of forum shopping and

regulatory arbitrage. To address this concern, the following two complementary recommendations are proposed:

1. **Setting up a standing committee for coordination with a schedule of meetings between EBA and the national authorities.** As part of this recommendation, the representative national supervisory authorities and EBA would form a standing committee with an annual schedule of meetings on PSD2 application issues. EBA and the national supervisory authorities would meet each other regularly and EBA would check national supervisory practices for PIs and EMIs, as well as the national application of PSD2 rules. EBA would regularly inform the Commission regarding schedule and outcomes; and

   Advantages: 1) uniform application of licensing and supervisory rules as well as of the Article 3 on the exemptions; 2) No further costs. The regulation n. 1093/2010/EU already vested EBA with these powers

   Risks: National authorities might not change their divergent interpretation and application of the PSD2 rules and "explain or comply" may not work as an approach in practice.

2. **Setting up a standing committee with a schedule of meetings among the central banks of the ESCB.** Under this recommendation, the representatives of national central banks of the eurozone and the ECB would form a standing committee with an annual schedule of meetings on PSD2 application issues.

   Advantages: 1) uniform application of art. 127 TFEU and normative powers of the oversight functions; 2) no further costs: the ESCB and its members are already vested with the oversight powers; 3) no revision of the Treaty.

   Risks: National authorities might not stick with the common interpretation approach chosen together.

Address competition issues. While PSD2 of course applies without prejudice to the application of competition law, including the Digital Markets Act (DMA), the report has shown that under the current PSD2 rules, BigTechs leverage network effects (due to their access to non-payments related data, existing customer base, technology), which could create market powers that may prevent or distort competition. In addition, there are different national approaches to the surcharging ban. To address these issues the following recommendations are proposed:

1. **Scheduling continued antitrust scrutiny to ensure effective competition investigations on overdraft conditions**
2. **Regularly informing the European Parliament on the results of the investigations on Big Techs carried out at the national level**
3. **Creating a public and distributed register with the results of the antitrust investigations**
4. **Scheduling regular meetings between the ECB, NCBs and the network of antitrust authorities**
5. **Addressing the operation of (retail) payment systems as a regulated business**
6. **Setting up an information structure (i.e. a list, ledger or map) on Member State choices on surcharging to establish which Member States used/did not use the option available within the PSD2**

   Advantages: the Recommendations do 1) not have further costs: the NAAs are already vested with the investigation power; 2) there is no need to amend the PSD2; 3) and the recommendations together will lead to greater transparency in the application of the PSD2 rules.

   Risks: it is likely that these recommendations will engender criticism from big players in the market who might dispute the risk of competition distortion. In addition, there is a risk that national central banks and antitrust authorities may cooperate with these actions, and it will be important to build a support for coordinated action.

Address legal uncertainty about the scope of PSD2 and the applicable rules as a result of new value chains and payment processes created by new technological solutions. In the first instance, this will require working on the definitions within the PSD2 by building on the existing PSD2 text. This should start from a general definition of "payment service", which should describe the key features of a payment service compared with other financial services, as well as services ancillary to the execution of payments which are not covered in the PSD2. Clarifying the definition of a payment service should reduce ambiguities and help with consistency in application in the face of new technological solutions that have fostered the rise of digital payments and are accelerating the move to cashless payments. To address this, the following recommendations are proposed:

1. **Inserting a residual normative clause in the PSD Annex on payment services**
2. **The residual normative clause would have a broad scope that does not exclude any future PIS/AIS-like services and it would cover both funds and data associated with fund transfers/custody as well as monetary value memorised as e-money**
3. **Guidelines and coordination activity by EBA on the approach to the residual normative clause**

Advantages: the introduction of a residual normative clause enables the rules to remain up to date with technological developments, comply with the original choice of a directive as a legislative tool (rather than moving to a regulation), reduce the risk of technological aging of the PSD2 and the risk of inconsistent interpretation and application of the PSD2 by national authorities when new technological solutions are concerned

Risks: there may be a risk of forum shopping if EBA coordination activity does not work properly

Address legal uncertainty within the PSD2 which is a large cost item for market participants and leads to an uneven playing field. There is a need for close interplay between PSD and MICA and future regulation of CBDCs because of the impact that CBDCs and crypto-assets will have on cross-border payments and the competition between payment methods. At the same time, consumer protection needs might have to be rethought given these methods of payments. To address these issues, the following recommendations are proposed:

1. **Establishing a legislative consolidation process between MICA and PSD2**
2. **Revising the definition of funds in the PSD2 to cover e-money tokens**
3. **Adding "quasi-fund" definition to cover asset-referenced tokens**
4. **Inserting a chapter in the PSD2 title on PSPs covering authorisation and supervision of issuers of asset referenced token issuers and e-money token issuers**
5. **Extending the application of the information requirements also to payment transactions by means of e-money tokens and asset-referenced tokens**
6. **Excluding the application of Title IV to payment transactions by e-money tokens and asset referenced tokens**

Advantages: the Recommendations may make PSD application more effective

Risks: the Recommendation may raise critical reactions from crypto-asset issuers and there is a need to revise the MICA regulation proposal

Unify PSD2 and EMD2 to address legal uncertainty and diverging application of rules across countries and for different market participants. To address this a legislative consolidation between the two texts is proposed by

1. **Adding a chapter on the authorisation and supervisory requirements for electronic money institutions in the PSD3 Title on PSPs**
2. **Extending the application of Titles III and IV of the PSD2 to e-money payment transactions**
3. **Removing preamble (6) of EMD2**

4. **Setting a single set of core definitions applicable both to e-money and payment services**

   Advantages: these changes will make PSD/EMI2 application more effective and reduce one of the largest cost items linked to PSD2 (i.e., legal uncertainty and interpretation)

   Risks: it will take significant time to frame a consistent legal text

Adopt more consistent definitions of the following main issues: access to accounts (within the PSD+EMD), access to payment systems (better within the FSD), agents/outsourcing (within the PSD+EMD).There are divergent approaches at national level to the "agent" exemption; divergent application practices for direct and indirect access of EMI and PIs to payment system which creates legal uncertainty, slows the development of the cross-border payments and represents a market barrier. To address this, the following recommendations are proposed:

1. **EBA guidelines on the "agent" exemption on a regular basis**
2. **EBA guidelines on the indirect access of EMIs and PIs to payment systems**
3. **Consolidating the guidelines, PSD provisions and Q&As on "access to accounts" in the ASPSPs-TPPs relationship**
   Advantages: these suggestions aim to reduce legal uncertainty as one of the main cost items linked to PSD and they will remove some of the market barriers identified in the study

   Risks: the national supervisory authorities could not comply with EBA guidelines and there may be critical reactions among banks

Strengthen cooperation between national supervisory authorities over payment platforms and digital platforms providing payment services to prevent divergent application of PSD2 and divergent supervisory practices. This will reduce legal uncertainty about PSD2 rules and reduce costs for businesses. To address this, the following recommendations are proposed:

1. **Giving a legal framework to digital platforms providing payment services (for example: Amazon; Apple Pay, and so on) as foreseen in the DMA; and**
2. **Setting up a supervision committee of platforms on a cross-border basis coordinated by EBA**

Under this recommendation, the members of national supervisory authorities where the business platform operates join the committee chaired by EBA. They meet regularly and coordinate regulatory approaches and supervisory practices.

Advantages: it is anticipated that this recommendation will lead to more effective supervision thanks to the NCAs proximity, it will reduce the risk of regulatory arbitrage and engender a higher level of stability in the market

Risks: there may be a critical reaction from BigTech companies that are affected by the recommendation and it will be time-consuming

Recommendations on open banking

Address standardisation and interoperability issues, at least when it comes to QR code, card-payment payment transactions, and API standards as these present a risk of legal fragmentation. To address these issues the following recommendations are proposed:

1. **In the eurozone, vesting the European Payment Council with a coordinating task**
2. **Establishing a SEPA-like incentive mechanism to make businesses cooperate on the regulatory and technical standards (i.e. Open Banking, QR codes, APIs and so on).**

Advantages: the proposed approach complies with the PSD2's neutrality principle and no new pieces of legislation are needed at the EU level as this follows a bottom-up approach to regulation.
Risks: the processes of coordination and building cooperation is time-consuming and will not yield immediate results.

Ensure that emerging payment service providers are covered by the regulatory framework governing retail payments in the EU to maintain the effectiveness of the PSD2 in the future. To address this, the following recommendations are proposed:

1. **Defining a three-tier "payment service" concept based on i) the transfer and custody of monetary assets (i.e., funds) as well as what is preliminary to send or receive funds, ii) the transfer and custody of data associated with the payment transactions, iii) the managing of payment platforms.**
2. **Fostering closer cooperation among national authorities via EBA**
   Advantage: making the PSD more flexible and effective; complying with neutrality principle

   Risks: risk of legal uncertainty

Address FinTech industry concern that the implementation of PSD2 raises a range of obstacles and challenges that might affect the level playing field and effective competition. To address this, the following recommendation is proposed:

1. **amending Article 97 of PSD2 to make it clear that once a payment service user authorises an AIS to access its payment accounts (through a mandate for instance), then that permission is valid on an ongoing basis until the user revokes access.**

Recommendations on data protection and consumer protection

Set a more efficient data authorisation and customer identity control system to reduce the PSD-based cost items linked to legal uncertainty. To address this, the following recommendation is proposed:

1. **Improving coordination between EBA and data protection authorities.**

   Advantages: these recommendations will lower the costs of PSD application and increase the level of user protection

   Risks: need to update legislation regularly due to technological development

Improve protection of payment service users in the context of growing cashless payment systems and the need to improve outcomes for users and trust in new payment methods. To address these issues the following recommendations are proposed:

1. **Setting different levels of protection and liability based on the user's degree of vulnerability (for example, elderly people)**

   Advantages: making the cashless society more sustainable; dealing with different levels of financial and IT education of payment service users
   Risks: legal uncertainty throughout the Member States
2. **Increasing the effectiveness of cross-border ADR mechanisms (FIN-NET) for cross-border disputes on rights and obligations for payment services**

   Advantages: higher level of user protection; customer mobility; improving level playing field
3. **Extending the existing data protection safeguards in the PSD2, information requirements and fund protection to all payment services, with no differences across legal forms of the PSP**

Advantages: higher level of user protection
Risks: more costs for SMEs providing payment services

4. **Considering the business entity providing licence-as-a-service liable for the custody/transfer of funds/data in the relationship with the supervisory authority and for money laundering control because it made possible the business activity of any ASPSPs using its licence**

   Advantages: managing the risk of PSD sidestepping
   Risks: potential critical reaction from licence-as-a-service providers

5. **Streamlining the legal framework for information requirements by introducing one Title in the PSD covering information duties for PIs, EMIs; issuers of asset-referenced and e-money tokens**

   Advantages: higher levels of legal certainty; better level playing field
   Risks: time consuming because it requires to revise the MICA regulation proposal and remove duplications

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

– by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

– at the following standard number: +32 22999696, or

– by email via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications from: https://op.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1952 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

Open data from the EU

The EU Open Data Portal (http://data.europa.eu/euodp/en) provides access to datasets from the EU. Data can be downloaded and reused for free, for both commercial and non-commercial purposes.

EV-04-23-061-EN-N

ISBN 978-92-76-62087-7
DOI: 10.2874/996945