Council of the
European Union

Brussels, 5 July 2023
(OR. en)

11222/23
ADD 2

Interinstitutional File:
2023/0210 (COD)

EF 200
ECOFIN 694
CODEC 1237

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	29 June 2023
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2023) 231 final
Subject:	COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT Accompanying the documents Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on payment services in the internal market and amending Regulation (EU) No 1093/2010 and Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on payment services and electronic money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC

Delegations will find attached document SWD(2023) 231 final.

Encl.: SWD(2023) 231 final

EUROPEAN
COMMISSION

Brussels, 28.6.2023
SWD(2023) 231 final

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT REPORT

Accompanying the documents

Proposal for a
REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
on payment services in the internal market and amending Regulation (EU) No 1093/2010

and

Proposal for a
DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
on payment services and electronic money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC

{COM(2023) 366 final} - {COM(2023) 367 final} - {SEC(2023) 256 final} - {SWD(2023) 232 final}

Table of Contents

1. INTRODUCTION: POLITICAL AND LEGAL CONTEXT 1
1.1 Retail payments in the EU 1
1.2 Legal context.....4
1.3 Political context 6
2 PROBLEM DEFINITION 7
2.1 What is/are the problems and the problem drivers?.....7
2.1.1 Consumers at risk of fraud and lacking confidence in payments……8
2.1.2. Imperfect functioning of Open Banking……...12
2.1.3. Inconsistent powers and obligations of supervisors……16
2.1.4. Unlevel playing field between banks and non-bank PSPs ……..18
2.2. What are the consequences of the problems? 19
2.3. How likely is the problem to persist? 21
2.4. Problem Tree.....22
3. WHY SHOULD THE EU ACT?.....23
3.1. Legal basis 23
3.2. Subsidiarity: Necessity of EU action 23
3.3. Subsidiarity: Added value of EU action 23
4. OBJECTIVES: WHAT IS TO BE ACHIEVED?.....24
4.1. General objectives.....24
4.2. Specific objectives 24
5. WHAT ARE THE AVAILABLE POLICY OPTIONS?.....25
5.1. What is the baseline from which options are assessed?.....25
5.2. Description of the policy options.....26
5.2.1. Strengthen user protection against fraud and abuses…….. 26
5.2.2. Improve the competitiveness of Open Banking services……..29
5.2.3. Improve enforcement and implementation in Member States……..32
5.2.4. Improve (direct or indirect) access to payment systems and bank accounts for non-bank PSPs……...33
6. WHAT ARE THE IMPACTS OF THE POLICY OPTIONS AND HOW DO THEY COMPARE?.....35
6.1. Strengthen user rights and protection against fraud.....35
6.2. Improve the competitiveness of Open Banking services 40
6.3. Improve enforcement and implementation in Member States 48

6.4. Improve (direct or indirect) access to payment systems and bank accounts for non-bank PSPs....50
7. PREFERRED OPTIONS....52
7.1. Effectiveness....53
7.2. Efficiency....54
7.3. Coherence....56
7.4. Summary of preferred options....58
7.5. Other relevant impacts....58
7.6. Application of the 'one in, one out' approach....59
7.7. Climate and sustainability....59
7.8. Fundamental rights....59
7.9. REFIT (simplification and improved efficiency)....59
8. HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED?....60
ANNEX 1: PROCEDURAL INFORMATION....61
ANNEX 2: STAKEHOLDER CONSULTATION....63
ANNEX 3: WHO IS AFFECTED AND HOW?....83
ANNEX 4: ANALYTICAL METHODS....92
ANNEX 5: EVALUATION REPORT....98
ANNEX 6: SCOPE OF PSD2....161
ANNEX 7: TECHNICAL CLARIFICATIONS AND OTHER CHANGES....167
ANNEX 8: INTEGRATION OF THE E-MONEY DIRECTIVE 2 INTO PSD2....175
ANNEX 9: ACCESS TO CASH....179
ANNEX 10: USER RIGHTS MEASURES....182
ANNEX 11: EXPLANATORY NOTE ON OPEN BANKING....188
ANNEX 12: COHERENCE WITH OTHER COMMISSION ACTS AND INITIATIVES....197
ANNEX 13: SME TEST....202

Glossary

Term	Definition
Account Information Service (AIS)	In Open Banking, an online service to provide consolidated information on one or more payment accounts held by a payment service user with one or more payment service providers.
Account Information Service Provider (AISP)	A PSP which is authorised to access a user's account data at several account servicing PSPs and centralise it for the user in order to provider account information services.
Application Programming Interface (API)	A collection of software functions and procedures that allows different applications to communicate and exchange data, e.g. when a TPP requests account information of a user at an Account Servicing Payment Service Provider (ASPSP). Commonly used in Open Banking.
Account Servicing Payment Service Provider (ASPSP)	A PSP (for example a bank) which offers customers payment accounts and payment services (not a PSP which only carries out Open Banking services nor a PSP which only executes payments for its own account, not for customers). An ASPSP is a data holder in Open Banking terms.
Authorisation	The consent given by a participant (or a third party acting on behalf of that participant) in order to transfer funds or securities.
Automated teller machine (ATM)	An electromechanical device that allows authorised users, typically using machine-readable plastic cards, to withdraw cash from their accounts and/or access other services (allowing them, for example, to make balance enquiries, transfer funds or deposit money).
Card (payment card)	A category of physical portable payment instrument, with a magnetic stripe and usually a microchip, that enables the payer to initiate a debit or credit card transaction. Types of payment card include credit cards and debit cards.
Cardholder	A person to whom a payment card is issued and who is authorised to use that card.
Card issuer	A PSP contracting to provide a payer with a card payment instrument to initiate and process the payer's card-based payment transactions.
Card scheme	A technical and commercial arrangement set up to serve one or more brands of card which provides the organisational, legal and operational framework necessary for the functioning of the services marketed by those brands.
Cheque	A written order from one party (the drawer) to another (the drawee; normally a bank) requiring the drawee to pay a specified sum on demand to the drawer or a third party specified by the drawer.
Consumer (of payment services)	Any natural person who requests and makes use of a payment account for purposes other than his trade, business, craft or profession.
Contingency mechanism	In Open Banking, the online direct customer interface between PSUs and their ASPSPs, when made available to TPPs when the dedicated interface is not performing. Also known as "fallback".
Credit institution/ bank	A category of PSP authorised to carry out all banking transactions (i.e. to receive deposits from the public, carry out credit transactions, make funds available on loan and manage means of payment).
Credit transfer	A payment service for crediting a payee's payment account with a payment transaction or a series of payment transactions from a payer's payment

	account by the payment service provider which holds the payer's payment account, based on an instruction given by the payer.
Cross-border payment (transaction)	A payment transaction initiated by a payer or by a payee where the payer's PSP and the payee's PSP are located in different Member States or third countries
Cross-border payments Regulation (CBPR)	Regulation (EU) 2021/1230 of the European Parliament and of the Council of 14 July 2021 on cross-border payments in the Union
Digital Operational Resilience Act	Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector
Direct debit	A payment service for debiting a payer's payment account, where a payment transaction is initiated by the payee on the basis of the consent given by the payer to the payee, to the payee's payment service provider or to the payer's own payment service provider
Electronic money (e-money)	A monetary value, represented by a claim on the issuer, which is: 1) stored on an electronic device (e.g. a card or computer); 2) issued upon receipt of funds in an amount not less in value than the monetary value received; and 3) accepted as a means of payment by undertakings other than the issuer
Electronic Money Directive (EMD)	Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of E-Money Institutions
Electronic money institution (EMI)	A type of PSP which is not a bank, authorised and supervised under the Electronic Money Directive, whose activity is limited to the issuance of electronic money and the provision of financial and non-financial services closely related to the issuance of electronic money, including payments.
European Payments Council (EPC)	A private law association of banks and other payment service providers, founded in 2002 with the main task of the development of the Single Euro Payments Area, and which manages schemes for credit transfers and direct debits in euro, SCT and SDD.
Impersonation fraud	A type of fraud where a payment services user who is a consumer was manipulated by a third party pretending to be an employee of the consumer's payment service provider using lies or deception such as the bank's name and/or telephone number and this manipulation gave rise to subsequent fraudulent payment transactions.
Interchange fee	A fee paid for a transaction directly or indirectly (i.e. through a third party) between the issuer and the acquirer involved in a card-based payment transaction. The net compensation or other agreed remuneration is considered to be part of the interchange fee.
General Data Protection Regulation	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
International Bank Account Number (IBAN)	The standard governing European bank account numbers, compliant with ISO-13616, considered to be a "unique identifier" of a payment account
Interoperability	A set of arrangements/procedures that allows participants in different systems to conduct and settle payments or securities transactions across systems while continuing to operate only in their own respective systems.
Means of payment	Assets or claims on assets that are accepted by a payee as discharging a payment obligation on the part of a payer vis-à-vis the payee.
Markets in Financial Instruments Directive	Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments

Mobile payment	A payment where a mobile device is used at least for the initiation of the payment order and potentially also for the transfer of funds.
Money remitter	A payment service provider that accepts funds from a payer for the purpose of making them available to a payee, without necessarily maintaining a payment account for the payer or payee.
Open Banking	A framework for allowing payment service users to share their account data with Third Party Providers of payment-related services such as AISPs and PISPs
Open Banking permissions dashboard	A graphic interface which provides a customer with an overview of active data sharing permissions and to which parties, and which allows the customer to manage the permissions for data sharing.
Payer	A natural or legal person who holds a payment account and allows a payment order from that payment account, or, where there is no payment account, a natural or legal person who gives a payment order.
Payee	A natural or legal person who is the intended recipient of funds which have been the object of a payment transaction.
Payment Initiation Services (PIS)	In Open Banking, a service offered by a PISP to initiate a payment order at the request of a payment service user with respect to a payment account held at another account servicing payment service provider
Payment Initiation Services Provider	In Open Banking, a category of PSP which is authorised to access a PSU's payment account at an ASPSP to initiate an account-to-account payment order.
Payment institution	A type of PSP which is not a bank, authorised and supervised under Title II of PSD2, to provide and execute payment services throughout the Union.
Payment instrument	A tool or a set of procedures enabling the transfer of funds from a payer to a payee. The payer and the payee can be one and the same person.
Payment scheme	A single set of rules, practices, standards and/or implementation guidelines agreed between PSPs for the execution of payment transactions across the Union and within Member States, and which is separated from any infrastructure or payment system that supports its operation.
Payment service	Any of the categories of payment services listed in Annex 1 of PSD2: 1. Services enabling cash to be placed on a payment account as well as all the operations required for operating a payment account. 2. Services enabling cash withdrawals from a payment account as well as all the operations required for operating a payment account. 3. Execution of payment transactions, including transfers of funds on a payment account with the user's payment service provider or with another payment service provider: 4. Execution of payment transactions where the funds are covered by a credit line for a payment service user: 5. Issuing of payment instruments and/or acquiring of payment transactions. 6. Money remittance. 7. Payment initiation services. 8. Account information services.
Payment Service Provider (PSP)	An entity registered to provide payment services. Generally, PSPs can be: – credit institutions; – payment institutions; – E-Money Institutions; – post office giro institutions; – others, e.g. public authorities or national central banks (in some cases).

Payment service user (PSU)	A natural or legal person making use of a payment service in the capacity of payer, payee, or both.
Payment transaction	An act, initiated by the payer or by the payee of transferring funds, irrespective of any underlying obligations between the payer and the payee.
Payment system	A funds transfer system with formal and standardised arrangements and common rules for the processing, clearing or settlement of payment transactions.
PIN (Personal Identification Number)	A personal and confidential numerical code which the user of a payment instrument may need to use in order to verify his/her identity.
POND principle	The principle, laid down for example in article 35.1 of PSD2, that rules must be Proportionate Objective and Non-Discriminatory
Second Payment Services Directive (PSD2)	Directive 2015/2366 of 25 November 2015 on payment services in the internal market
PSD2 Regulatory Technical Standard (RTS)	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[1]
Remote payment	Defined in PSD2 (art. 4(6)) as "a payment transaction initiated via internet or through a device that can be used for distance communication"
Retail payment	Payments both initiated by and made to individuals or non-financial companies.
Settlement Finality Directive (SFD)	Directive 98/26/EC of 19 May 1998 on settlement finality in payment and securities settlement systems
Single Euro Payments Area (SEPA)	An initiative of European banks and the Eurosystem and European Commission with a view to integrating retail payment systems and transforming the euro area into a true domestic market for the payment industry.
Strong Customer Authentication (SCA)	Authentication of an operation using at least two of the following three elements: something the user knows (e.g. password or PIN), something the user has (e.g. mobile phone or hardware token), something the user is (e.g. fingerprint or face recognition).
Third Party Provider of payment services (TPP)	A non-account-servicing PSP carrying out Open Banking services, either payment initiation services or account information services (an AISP or a PISP). A TPP is a data user in Open Banking terms.

[1] While this is not the only Regulatory Technical Standard under PSD2, it is the only one discussed in this impact assessment.

Table of Abbreviations

ADR	Alternative Dispute Resolution
AIS	Account Information Service
AISP	Account Information Services Provider
AML	Anti-Money Laundering
APP	Authorised Push Payment
ART	Asset-referenced token
ASPSP	Account Servicing Payment Service Provider
ATM	Automatic Teller Machine
CASP	Crypto-assets service provider
CJEU	Court of Justice of the European Union
CSC	Common and Secure Communication
DORA	Digital Operational Resilience Act
EBA	European Banking Authority
EDIW	European Digital Identity Wallet
EEA	European Economic Area
ECB	European Central Bank
EEA	European Economic Area
EMD	Electronic Money Directive
EMI	Electronic Money Institution
EMT	Electronic Money Token
ERPB	Euro Retail Payments Board
EPC	European Payments Council
GDPR	General Data Protection Regulation
IBAN	International Bank Account Number
ICT	Information and Communication Technology
IFR	Interchange Fee Regulation (Regulation (EU) 2015/751)
IP	Instant Payment
IT	Information Technology
MFI	Monetary Financial Institution
MiCA	Markets in Crypto Assets Regulation
MiFID	Markets in Financial Instruments Directive
MIT	Merchant Initiated Transaction
MOTO	Mail Order or Telephone Order

NCA	National Competent Authority
NFC	Near Field Communication
OBIE	Open Banking Implementation Entity (in the UK)
P2P	Peer to peer
PI	Payment Institution
POI	Point of Interaction
POS	Point of Sale
PSD2	Second Payment Services Directive
PSMEG	Payment Systems Market Expert Group
PSP	Payment Service Provider
PSU	Payment Service User
QR	Quick Response
RPS	Retail Payments Strategy
RTS	Regulatory Technical Standard(s)
SCA	Strong Customer Authentication
SCT	SEPA Credit Transfer
SDD	SEPA Direct Debit
SEPA	Single Euro Payments Area
SFD	Settlement Finality Directive
TMM	Transaction Monitoring Mechanism(s)
TPP	Third Party Provider
TRA	Transaction Risk Analysis

1. INTRODUCTION: POLITICAL AND LEGAL CONTEXT

1.1 Retail payments in the EU

Retail payments are the lifeblood of the European economy. Effective and efficient retail payment systems are essential for the smooth running of multiple sectors, the retail sales sector, payments for utilities and rent, and many others, as well as payments between individuals and between businesses. The second Payment Services Directive (PSD2) entered into force in 2018 (replacing PSD1 which dated from 2007) and lays down the EU legal framework for retail payments[2]; since 2018, the retail payment services market has been undergoing key changes largely related to the increasing use of cards and other digital means of payment, and the growing presence of new players and services. The Covid-19 pandemic and the transformations it brought to consumption and payment practices has heightened the importance of secure, efficient digital payments.

Payment Service Users (PSUs, consumers and businesses), receive payment services from Payment Service Providers (PSPs, mostly banks, but increasingly Payment Institutions and E-Money Institutions, neither of which is allowed to lend money, unlike banks, and also international remittance specialists). Some PSPs provide payment accounts (these are known as ASPSPs, Account Servicing PSPs), while others provide payment services without the need for an account (these include Open Banking providers, Account Information Service Providers and Payment Initiation Service Providers, collectively known as Third Party Providers or TPPs). Digital means of payment include credit transfers, direct debits, card-based payments, e-money stored in digital wallets, and newer innovative means of payment, such as using crypto-currencies. All digital payments require IT infrastructures in order to operate, including different phases of a digital payment, such as authorisation, initiation, execution and settlement. Some payment systems are entirely private, while public sector bodies such as the Eurosystem operate certain key infrastructures. While cash itself is not a digital means of payment, obtaining cash, for example from an ATM, is a digital payment service requiring an IT network. Non-digital means of payment, such as cheques, still persist in some Member States, despite high costs and inefficiencies.

Reaching €240 trillion in 2021 (compared with €184.2 tn in 2017), cashless payments in the EU have been in constant growth, both in number and value of transactions (see Figure 1). They are also increasing as a percentage of all payments, as shown in an ECB study[3]. According to this study, in 2022, cash was used in 59% of Point Of Sale (POS) transactions in the euro area, down from 79% in 2016[4]. While cards represented 34% of POS transactions (up from 19% in 2016), in terms of value, they accounted for a higher share of transactions

---

[2] "Retail payments" designates the use of non-cash payment instruments by consumers and non-financial businesses, including cards, credit transfers, direct debits, e-money and cheques.

[3] ECB 2022 Study on the payment attitudes of consumers in the euro area (SPACE) builds on data collected through a survey of a random sample of the population in all euro area countries. It follows an identical SPACE from 2020 and 2016 study on the use of cash by households in the euro area (SUCH).

[4] Esselink, H. and Hernández, L., The use of cash by households in the euro area, ECB Occasional Paper Series, No 201, November 2017.

than cash (46% compared to 42%), a change from 2019, when cash accounted for a higher share of value of payments than cards (47% compared to 43%).

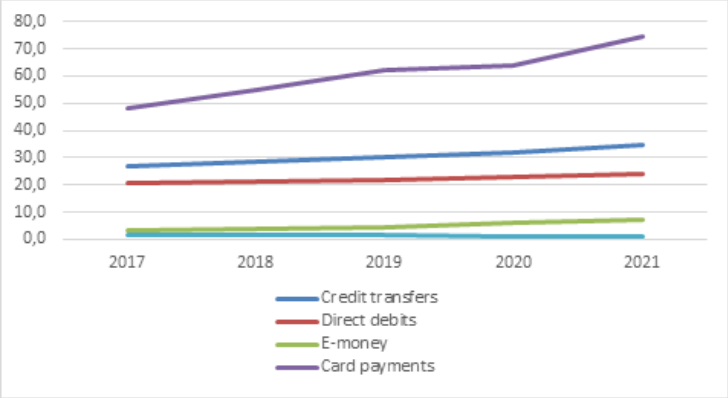
Figure 1: Cashless payments in the EU

	2015	2016	2017	2018	2019	2020	2021
Total number (bn)	114.3	123.2	128.1	139.7	152.0	126.9	143.2
Total value (€ tn)	276.7	281.4	289.3	282.8	290.3	202.0	239.9

Source: ECB Statistical Data Warehouse; figures for EU (changing composition), all currencies combined

Amongst cashless payments, a number of important trends have occurred in recent years, resulting from digitisation of the economy, diversification in the supply of means of payment, changes in payment habits, etc. As illustrated below (Figure 2), despite the increase in both credit transfers and direct debits, the most noteworthy trends are the increasing use of cards (with a 55% increase in 2021 compared to 2017) and e-money (120% increase in 2021 compared to 2017).

Figure 2: Number of cashless payments in the EU 2017 - 2021 (in billions)



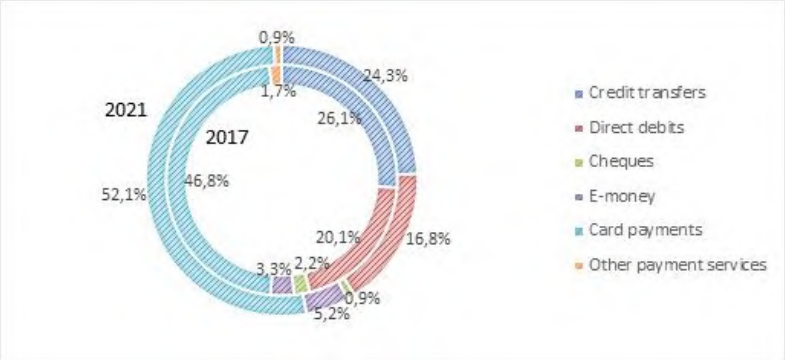
Source: ECB Statistical Data Warehouse; Payment Statistics 2021

In percentage terms, cards rose to 52% of total number of transactions (compared to 46.8% in 2017), and e-money payments to 5.2% (up from 3.3% in 2017), whereas the share of other payment instruments has fallen (see Figure 3)[5]. However, there are variations between Member States. Thus, for instance, the share of card payments stood well above 52% in Portugal (72,2%) and Romania (71,8%), where it has not changed significantly compared to 2017. The use of cards was also below the EU average in Germany (30,3%) and Bulgaria

[5] ECB, Statistical Data Warehouse, Payments Statistics Report, July 2022.

(35%), although in both cases these figures represent an increase of about 10 percentage points. when compared to 2017.

Figure 3: Relative importance of various payment instruments (as percentage of the total number of payments) 2017 and 2021



Source: ECB Statistical Data Warehouse; Payment Statistics 2021

These trends have been influenced by changes in behaviour, but also by a growing diversity of providers of payments as well as technical services. COVID-19 accelerated the rise of e-commerce. In 2020, 22% of EU companies had e-commerce sales, with 19% of them reporting that online sales reached at least 1% of their total turnover, a 1 percentage point (pp) increase compared with 2019 and 6 pp up from 13% in 2010[6]. In 2021, card payments were the most used payment method in e-commerce: credit cards accounted for 25% and debit cards for 17% of the total e-commerce transaction value in the EU[7]. Card payments were followed by mobile wallets, which represented 27% of the transaction value in 2021.

New players enabled by digital technologies have become more widely available to consumers. For example, non-bank Payment Service Providers (PSPs) such as Payment Institutions (PIs) and E-Money Institutions (EMIs) are now widely present in the market, with the EBA's register of payment and E-Money Institutions under PSD2 presenting 724 PIs and 275 EMIs in 2022[8]. In addition, more efficient payment systems have recently been developed, notably permitting instant credit transfers, taking place within seconds. According to data from the European Payments Council for Q3 2022, instant payments (IPs) account for about 13% of total volume of euro credit transfers in the EU.[9]

Finally, related to the growing use of mobile phones for payments, large technology companies ('BigTechs') have become more prominent in the payments sector as technology

[6] Eurostat, Online sales continue to grow among EU enterprises, December 2021.
[7] *Ibid.*
[8] European Banking Authority, Register of payment and E-Money Institutions under PSD2.
[9] European Payments Council, SCT Inst scheme – where are we now and where are we heading?

or payment service providers, particularly via pass-through digital wallets enabling access to tokenised versions of payment cards allowing contactless payments. Benefitting from significant network economies and from their large access to non-payments data, they can challenge established providers. Crypto-assets (including so-called 'stablecoins') may in future increase their role in retail payments by offering new payment solutions based on encryption and distributed ledger technology (DLT), although crypto-assets are not currently used on any significant scale for retail payments.

1.2 Legal context

The second Payment Services Directive (PSD2) since 2018 provides a framework for all retail payments in the EU, Euro and non-Euro, domestic and cross-border. The first Payment Services Directive (PSD1), adopted in 2007[10], aimed at establishing a harmonised legal framework for the creation of an integrated EU payments market. By removing the legal and technical obstacles to a single payments market as well as by promoting market entry by a new class of financial institutions, namely payment institutions, PSD1 aimed at introducing more competition in payment systems and facilitating economies of scale. PSD1 also provided a set of rules with regard to information requirements and reinforced the rights and obligations linked to payment services.

The second Payment Services Directive (PSD2), adopted in 2015 and replacing PSD1, aimed to address barriers to new types of payment services and improve the level of consumer protection and security[11]. Most of the rules in PSD2 have been applicable since January 2018, but some rules on SCA and access to payment accounts data have applied only since September 2019. In particular, PSD2 aimed to:

- ensure a level playing field between incumbent and new providers of card, internet and mobile payments;
- increase the efficiency, transparency and choice of payment instruments for payment service users (consumers and merchants);
- facilitate the provision of card, internet 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;
- ensure a high-level protection for PSUs across all Member States of the EU.

The review clause of PSD2 (Article 108) required the Commission to report on the application and impact of the Directive by 13 January 2021, in particular on charges, scope, thresholds and access to payment systems. The review could not take place by the date provided for in the Directive due to its late transposition by some Member States and the delay in applying some of its rules, such as on Strong Customer Authentication. The PSD2 evaluation therefore took place in 2022, including a call for advice to the EBA (hereafter the

[10] Directive 2007/64/EC of 13 November 2007 on payment services in the internal market .
[11] Directive (EU) 2015/2366 of 25 November 2015 on payment services in the internal market .

'EBA Advice')[12], a study by an external contractor (hereafter the 'VVA/CEPS study')[13], and various public and technical consultations (see Annex 2). The review report required by Article 108 is being submitted to the EU co-legislators together with the present initiative.

Another key piece of legislation in the payments area is the Single Euro Payments Area (SEPA) Regulation of 2012, which harmonises credit transfers and direct debits in euro[14]. On 26 October 2022, the Commission proposed an amendment to the SEPA Regulation, to accelerate and facilitate the use of euro Instant Payments in the EU[15].

A number of other relevant items of EU legislation exist in the payments area. Pricing of domestic and cross-border transfers in euro has been equalised by law[16]. Multilateral interchange fees for card payments have been regulated with maximum levels[17]. A legal framework for e-money has been laid down[18]. The Settlement Finality Directive[19] also covers certain payment systems and is relevant in the context of this impact assessment. Regarding crypto-assets, a Markets in Crypto-Assets Regulation (MiCA) was adopted by the co-legislators in 2023[20], and a Digital Operational Resilience Act concerning cyber-security (DORA) has been adopted[21].

For Open Banking (see Annexes 5 and 11 and section 2.1.2. below), which centres around the use of account data, which often constitute personal data, an important part of the legal framework is the General Data Protection Regulation (GDPR)[22] which provides for general rules and requirements to ensure free flow of personal data and ensures the protection of privacy and personal data of individuals in the EU. In February 2022, the Commission adopted a proposal for a Data Act, to regulate who can access and make economic use of data; when that proposal enters into force it will provide another key framework for Open Banking [23], alongside the future EU legal framework for Open Finance, concerning financial

---

[12] European Banking Authority (EBA/Op/2022/06) Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2), of 23 June 2022.
[13] FISMA/2021/OP/0002, A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2). Available here.
[14] Regulation (EU) No 260/2012 of 14 March 2012.
[15] COM(2022) 546 final. See Annex 12 for more information about this proposal.
[16] Regulation (EU) 2021/1230 of 14 July 2021 on cross-border payments in the Union (CBPR).
[17] Regulation (EU) 2015/751 of 29 April 2015 on interchange fees for card-based payment transactions.
[18] Directive 2009/110/EC of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of E-Money Institutions.
[19] Directive 98/26/EC of 19 May 1998 on settlement finality in payment and securities settlement systems.
[20] Regulation (EU) 2023/1114 of 31 May 2023 on markets in crypto-asssets. MiCA recognises one of the three categories of crypto-assets, namely e-money tokens, as funds in the meaning of PSD2.
[21] Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector. While PSPs in the meaning of PSD2 are covered by DORA, payment systems infrastructure operators are not covered but a review clause requires the Commission to reconsider this exclusion, in the context of the PSD2 review. See Annex 6 and Annex 12.
[22] Regulation (EU) 2016/679 of 27 April 2016 .
[23] Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act), COM/2022/68 final of 23 February 2022.

data other than payments data, for which a proposal will be presented by the Commission in parallel with the revision of PSD2.

The European Central Bank and the Eurosystem play an important role in payment systems regulation and oversight. For the oversight of payment systems the standards are mainly laid out in the Regulation on Systemically Important Payment Systems[24], and the oversight framework for retail payment systems (RPS), which are not systemically important. For payment instruments, schemes and arrangements the "PISA" oversight framework applies[25].

See section 7.6 and Annex 12 for coherence of this initiative with existing legislation and initiatives.

1.3 Political context

The proposed revision of PSD2 features in the Commission Work Programme (CWP) for 2023[26], along with a planned legislative initiative on Open Finance, extending financial data access and use beyond payment accounts to more financial services. The same CWP includes a package to strengthen the role of the euro, including legislation providing a legal basis for a future digital euro, a Regulation regulating the legal tender status and accessibility of cash.

The Commission's 2020 Communication on a Retail Payments Strategy (RPS) for the EU[27] laid down the Commission's priorities for the retail payments area for the present Commission college mandate. It was accompanied by a Digital Finance Strategy, setting out priorities for the digital agenda in the finance sector other than payments[28]. The RPS announced the launch of a comprehensive review of the application and impact of PSD2, "*which should include an overall assessment of whether it is still fit for purpose, taking into account market developments*". The RPS planned for the review to include, among other things, "*an assessment of risks stemming from unregulated payment services, a stocktaking of the impact of strong customer authentication on the level of payment fraud, and an assessment of the development of new business models based on sharing payment account data, such as payment initiation and account information services"*.

In its 2021 Conclusions on the RPS[29], the Council welcomed "*a comprehensive review of the implementation of the Payment Services Directive 2 (PSD2), after its full deployment and taking into account the challenges encountered in its implementation, focusing in particular on assessing: i) the appropriateness of the scope of application (including as regards technical service providers), and the need for further clarification of existing concepts and rules; ii) the interplay with other sectoral legislation, notably the E-money Directive, the Anti-money laundering Directive, the GDPR as well as ongoing legislative developments; iii)*

---

[24] ECB Regulation ECB/2014/795 of 3 July.
[25] Eurosystem oversight framework for electronic Payment Instruments, Schemes and Arrangements. November 2021
[26] COM/2022/548 final, of 18 October 2022.
[27] COM/2020/592 final, of 24/9/2020.
[28] COM/2020/591 final, of 24/9/2020.
[29] Council document 7225/21 of 22 March 2021. See §25ff.

the evolution to 'open banking', the handling of privacy-related risks, and the interplay with EDPB guidelines in that respect; iv) its impact on competition, including the increasing role of Big Tech and FinTech; v) its effectiveness in limiting fraud and enhancing consumer protection, including strong customer authentication (SCA)". The Council also "*supports an extension of the scope of the Settlement Finality Directive (SFD) to include e-money and payment institutions, providing that the potential risks are carefully assessed and adequately mitigated*".

The European Parliament did not adopt a report on the RPS, but on 17 March 2021 the Commission organised a webinar on the RPS with members of the ECON Committee. At that webinar, opinions of individual MEPs on the PSD2 review included the view that continued market fragmentation and obstacles to innovation must be addressed, that PSD2's future-proofing be ensured and that its scope must be broadened to cover new types of market participants, where justified.

2 PROBLEM DEFINITION

Based on its PSD2 evaluation the Commission services have identified certain areas where the objectives of PSD2 have not been fully achieved (see the Evaluation Report at Annex 5). For example, the evaluation analysis has identified the rise in new types of fraud as an issue of concern with regard to consumer protection objectives. Shortcomings have also been identified with regard to the objective of improving the market in open banking services by lowering market barriers faced by TPPs, while progress towards the objective of improving the provision of cross-border payment services has also been limited, largely due to inconsistencies in supervisory practices and enforcement across the EU. Finally, the evaluation has also identified factors stifling progress concerning the PSD2 objective of levelling the playing field between all PSPs. These issues have been grouped, for the purposes of this impact assessment, into four topics: i) payment user protection (notably against fraud); ii) functioning of Open Banking; iii) legal uncertainty and Single Market fragmentation due to imperfect implementation and enforcement of PSD2 and iv) access to key payment infrastructures by non-bank PSPs, leading to an unlevel playing field among PSPs.

Alongside these four areas discussed below in this section, a number of clarifications and technical changes to the Directive are also deemed necessary; these clarifications are described in Annex 7. No major changes to the Directive's scope are planned; this is explained in Annex 6. With a view to addressing the external coherence issues raised in the Evaluation Report, it is considered that the legislative frameworks concerning E-Money Institutions and Payment Institutions (today covered by separate directives) should be brought closer together and that the e-money Directive should therefore be repealed and its contents incorporated, with appropriate adjustments, into PSD; this is explained in Annex 8. The implications of PSD2 for cash distribution by non-banks (independent ATM operators and retailers), and modifications planned in this area, are discussed in Annex 9.

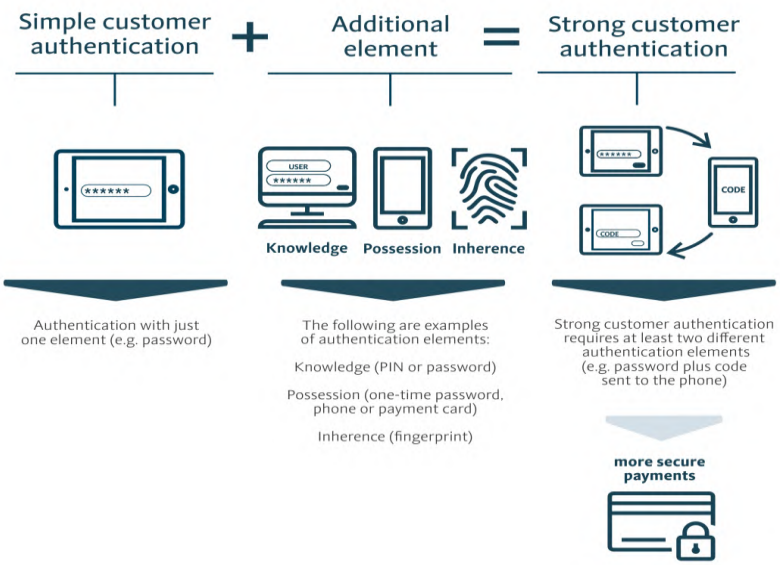
2.1 What is/are the problems and the problem drivers?

Given that the problem drivers are essentially regulatory (except for continuous development of new types of fraud), problems and drivers are discussed together in one section.

2.1.1 Consumers at risk of fraud and lacking confidence in payments

In the area of fraud, the major innovation of PSD2 was the introduction of SCA (Strong Customer Authentication). See Figure 4 below for the principles behind SCA, which involves two authentication measures, based on either knowledge (e.g. a password) or possession (such as a card) or inherence (such as a fingerprint). Article 97 of PSD2 requires PSPs to apply SCA where the payer accesses a payment account online, initiates a digital payment transaction, or carries out any action through a remote channel which may imply a risk of payment fraud or other abuses. The PSD2 regulatory technical standards on SCA and common and secure communication (hereafter, "the RTS")[30] introduced further security requirements applicable to PSPs. The Commission's evaluation (see Annex 5) concludes that SCA has already been highly successful in reducing fraud. However, a number of fraud-related issues remain.

Figure 4: Strong Customer Authentication (source: Bank of Portugal)



[30] 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 of 27 November 2017, as amended.

- *New types of fraud not prevented by SCA*

There are still fraud-related problems, despite the success of SCA in reducing fraud. One of the drivers of these is the fact that fraudsters are constantly adapting their techniques to get around regulatory frameworks. Such techniques can involve illegal impersonation (e.g. a fraudster makes the payment instead of a genuine payer as a result of a cyberattack or theft of a payment instrument), or a criminal activity which occurs before the payment is made by a genuine payer. Such "pre-payment fraud" can take the form of invoice fraud (where invoices are intercepted and the merchant account number is substituted for that of the fraudster[31]), or more sophisticated "Authorised Push Payment" (APP) frauds involving social engineering of the payer through direct interaction (e.g. manipulation of the payer into believing s/he is dealing with a genuine payee or even with a bank representative). Cases of such APP fraud (phishing, vishing, smishing, spoofing etc.) cannot be tackled by SCA because, technically and legally, most of these fraudulent transactions have been authorised by the payer using SCA. The fraud is in fact taking place before SCA without the payer knowing that s/he is being defrauded. The consumer thinks in good faith that s/he is sending money to recipient X, whereas in reality s/he is sending money to a fraudster. According to the European Payments Council, social engineering attacks and phishing attempts are still increasing, often in combination with malware, with a shift from consumers, retailers, SMEs to company executives, employees (through "CEO fraud" or "impersonation fraud"), payment service providers (PSPs) and payment infrastructures and more frequently leading to APP fraud. These techniques have greatly evolved over the last years as the targets are users rather than technology. In Ireland for example APP fraud rose by 15.9% in volume terms year on year in 2021 with an average APP fraud transaction amounting to € 4,237 in 2021[32]. According to Banque de France, APP fraud in France corresponds to 59% of total fraud in value terms[33]. In the UK in 2021, scams involving the impersonation of police or bank staff were the second-highest category in terms of value, with £137.3mn lost to these forms of fraud. This represented an increase of more than 50 per cent on 2020 levels[34]. In the Netherlands in 2022, reported cases of impersonation fraud amounted to € 51mn of which 89% was reimbursed to consumers on a voluntary basis via a leniency scheme that four major Dutch banks have signed up to[35].

Credit transfers have been found by the European Banking Authority (EBA)[36] to be the payment method for which APP fraud is the most prevalent, compared with other payment instruments (such as cards, for which the more common type of fraud involves making unauthorised payments, now substantially prevented by SCA). EBA stressed that credit transfers, due to the much higher average value of fraudulent transactions (€ 4 190), had the highest aggregate value of fraud (ca. € 310 million) in the second half of 2020, despite the

[31] On invoice fraud, see section 3.3. of the European Payment Council report « 2022 Payments Threats and Fraud Trends », available at this link.
[32] FraudSMART, Payment Fraud Report H2 2021, p. 4.
[33] Observatory for the security of payment means, Annual report 2021, July 2022, p. 7.
[34] 2022 UK Finance Annual Fraud Report, p. 64.
[35] Information provided by the Dutch Payments Association, 17 March 2023.
[36] European Banking Authority, Discussion Paper on the EBA's preliminary observations on selected payment fraud data under PSD2, as reported by the industry, EBA/DP/2022/01, January 2022.

lowest fraud rate overall; this generally translates to a significant impact on each affected customer, compared to other payment instruments. Based on fraud data collected by EBA[37] for 18 EEA countries, the average fraud rate for all credit transfers, in terms of value, in the second half of 2020 was 0.0011%, of which 43% was due to manipulation of the payer to initiate SCA-authorised transactions. On this basis the extent of APP fraud in 2020 for all SEPA euro credit transfers, including IPs, in the EU is estimated by the Commission at approximately € 323 million.

The problem is more common with respect to cross-border credit transfers (both inside and outside EEA), whose overall fraud rate exceeds that of domestic credit transfers by more than 20 times[38]. As a result, despite the fact that, according to the EBA analysis, cross-border credit transfers represented only around 2% of all credit transfers, their share in the total volume of credit transfer-related fraud reached 31% in the second half of 2020 for the 18 EEA countries.

Against this background, several stakeholders consulted in the context of the VVA/CEPS study on the application and impact of PSD2, including all types of market participants and national authorities, noted that there remain ways for fraudsters to circumvent security provisions. For example, fraudsters have found a way to slip into the SCA multiple layers, deceiving customers with false messages asking for personal information. EBA in its Advice considered that the legal framework does not fully mitigate the risks of social engineering fraud.

- *Abuse of SCA exemptions and of uncertainty about the scope of SCA*

PSD2 does not provide explicit clarity on whether some types of transactions are included or excluded from the application of SCA. This is the case of Mail Orders or Telephone Orders (MOTOs) and of Merchant Initiated Transactions (MITs). MITs are implicitly excluded from SCA by the fact that Article 97(1) of PSD2 applies SCA to three actions performed by the *payer*, not mentioning any payee-initiated actions. The Commission confirmed this through an EBA Q&A.[39] Regarding MOTOs specifically, recital 95 of PSD2 (the only place in PSD2 where MOTOs are mentioned) states that "*there does not seem to be a need to guarantee the same level of protection to payment transactions initiated and executed with modalities other than the use of electronic platforms or devices, such as paper-based payment transactions, mail orders or telephone orders"*.[40]

---

[37] Ibid.

[38] This higher rate of fraud for cross-border transactions exists for various reasons. For example, fraudsters often target cross-border transactions to take advantage of a less elaborated cross-border cooperation between Payment Service Providers and law enforcement agencies (for example taking stolen payment cards across a national border to carry out spending, or in cases of social engineering fraud, having a payment made to an account in a different Member State).

[39] European Banking Authority, Q&A 2018_4031 on the "Applicability of SCA to 'card payments initiated by the payee only'"

[40] Some guidance has been provided on the exclusion of MOTOs from the SCA requirements in Q&As. See EBA Q&As 2018_4058, 2019_4788, and 2019_4790.

As stated by EBA in its Advice,[41] "*the exclusion from the application of SCA for non-digital payment transactions has proved to be difficult to apply and supervise in practice based on the current formulation of Recital [95] since only cash payments would clearly fall outside the scope of SCA. All other types of payment transactions would in some part of the payment execution be handled electronically.*" EBA also noted in its Advice that "*the fraud levels and fraud risk related to the currently broad interpretation and application of MOTOs, based on feedback received from [competent authorities], are much higher than other payment transactions*" and that there is still a need to introduce in the Directive a clear definition of MOTOs and the specific requirements clarifying the situations that fall under the MOTO exclusion.[42] The VVA/CEPS study also notes that "*confusion has arisen whether MOTO is in or out of scope of the PSD2 SCA requirements*".[43]

EBA also notes in its Advice[44] the existence of issues of regulatory arbitrage between MITs and direct debits given the different regulatory approach between the two, notably in light of the 'unconditional' refund rights for SEPA direct debits, under Article 7 of the SEPA Regulation[45]. The Commission provided guidance on MITs via the EBA Q&As[46], notably on the applicability of SCA to '*card payments initiated by the payee only*'. However, in spite of this Q&A, the VVA/CEPS study notes that "*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".*[47] Some national authorities and trade bodies have also observed that "*there is strong evidence that MITs are sometimes used to circumvent SCA requirements*".

- *Consumer ignorance about fraud*

Consumer ignorance about fraud can also be a problem driver. Various respondents to the targeted consultation, including public authorities, but also the EBA in its Advice[48], note the importance of consumer literacy and education about fraud and the risks of certain payment instruments/methods, and that more effective awareness campaigns should be undertaken.

- *Insufficient cooperation between PSPs on fraud mitigation*

Another issue that has been recurrently flagged in the feedback received from stakeholders is inadequate cooperation between PSPs on their fraud mitigation strategies. ASPSPs and PISPs, for instance, have access to different data in the payment initiation process but do not necessarily share their insights with the other party in view of preventing fraud. The European Payment Council has argued[49] that an important aspect to mitigate risks and reduce fraud is the sharing of fraud intelligence and information on incidents amongst PSPs. Some

---

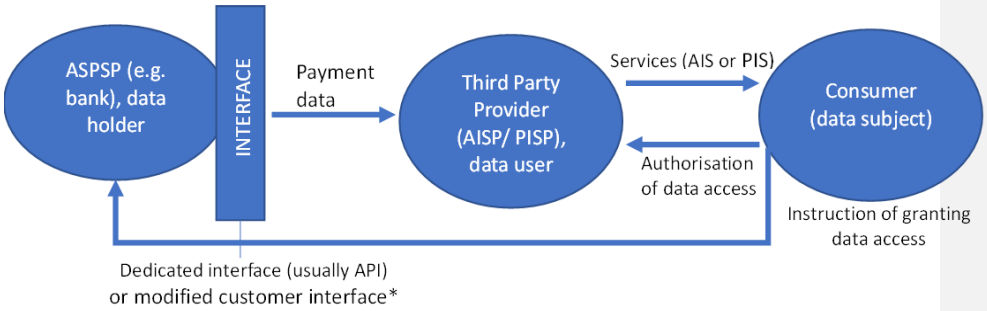
[41] Page 75. See reference at footnote 12 above.
[42] Ibid.
[43] VVA/CEPS study, page 145.
[44] Page 76, see reference at footnote 12.
[45] Regulation (EU) No 260/2012 of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro and amending Regulation (EC) No 924/2009.
[46] See footnote 39 above.
[47] VVA/CEPS study, page 145.
[48] Ibid, p.82.
[49] European Payments Council (EPC183-22), Report 2022 Payments Threats and Fraud Trends, November 2022

ASPSPs have explained that hesitancy exists because of concerns relating to compliance with GDPR and of their interpretations of the current AML framework does not allow them to share relevant information with PISPs. In some Member States, such as France, as noted by the French Banking Federation in its reply to the targeted consultation, the rules on banking secrecy prevent banks from sharing information.

2.1.2. Imperfect functioning of Open Banking

Open Banking (hereafter OB) is the term given to the process by which Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs), collectively known as Third Party Providers (TPPs[50]), provide value added services to users by accessing – with the user's consent - their account data held by other Payment Services Providers. Although this activity existed before PSD2, it operated in an unregulated way. PSD2 gave it a regulatory framework and imposed an obligation on account servicing payment service provider (ASPSP – mostly banks) to facilitate the access to payments data without any contractual obligations (i.e. for free), with the objective of both providing greater security and protection to users and of stimulating the development of OB to the advantage of users. Access to data is usually made available via APIs (Application Programming Interfaces), or by allowing TPPs to access the payments data directly via the same interface that banks use to interact with their customers directly (the customer-facing interface). See Annexes 5 and 11 for more details; a simple OB operation is illustrated in Figure 5 and a more complex one in figure 6 (other examples can be found in Annex 11).

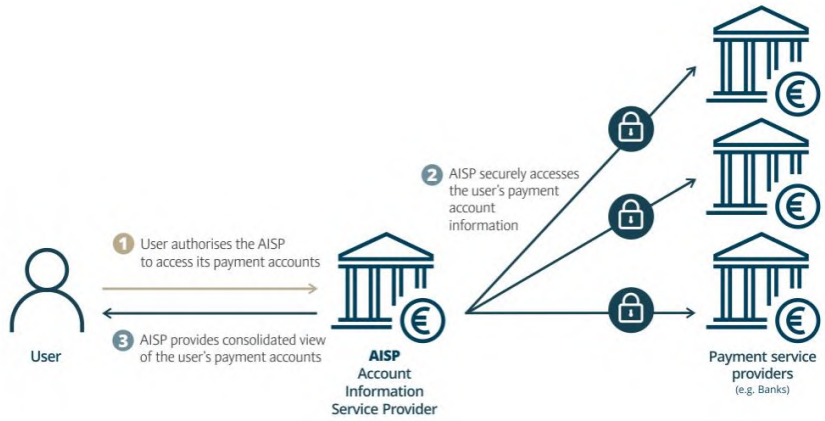
Figure 5: Open Banking simple case



* The modified customer interface is also known as the fallback interface or the contingency mechanism

[50] It should be noted that there are two different associations of TPPs in the EU, ETTPA and OFA. As a general rule, ETPPA members are TPPs which practiced Open Banking already before the PSD2 framework entered into force and tend to make more use of fallback interfaces, while OBA members have mostly been created after PSD2 and tend to prefer to use dedicated interfaces.

Figure 6: Account Information Service (source: Bank of Portugal)



To ensure business continuity for TPPs, PSD2 mandates ASPSPs that decide to implement a dedicated interface to make another interface available to TPPS (a fallback interface) in case the dedicated interface (API) is not functioning correctly. ASPSPs can apply to their NCA for an exemption from having to develop such fallback interface. This report will use "API" as standard terminology when discussing the dedicated interface. See annexes 5 and 11 for more details.

AIS providers can provide a user with aggregated and/or analysed information on the basis of their payment accounts, helping users to manage their finances or enabling users to receive a service, based on the data accessed, from another service provider (accountant, auditor, credit scoring bureau, etc.). PIS are account-to-account, non-card-based payments and can be found in e-commerce as one of the payment methods offered by a merchant. AIS and PIS both require the consent of the "payment service user" (PSU) to access the data on the user's payment account. Access, storage and use is limited to the data needed to perform the service explicitly consented by the PSU. AIS data can be particularly useful to help providers of PIS (PISPs) assess the risk of a payment initiated eventually not being executed.

As shown in annexes 5 and 11, the number of TPPs and the usage of OB has grown in Europe since PSD2 application, reaching almost 19 million in 2021[51]. Although consumer organisations and individual consumers have expressed concerns about data security in the context of Open Banking[52], the growth in the number of AISPs and PISPs would seem to indicate the existence of substantial demand. The legal framework has prevented ASPSPs

[51] Source: Statista, citing Juniper research. There are no official statistics on open banking in the EU (unlike in the UK), and data produced by private sector entities only give numbers for all of Europe including non-EU/EEA countries. Juniper forecasts the total number of open banking users in all of Europe to grow to 64 million by 2024 (see Figure 11 in Annex 5).
[52] See Annex 2 on public consultations.

from blocking TPPs' access to payment accounts (which was often the case in the pre-PSD2 era), and the security of users and their data has been achieved. PSD2's contribution to safe and secure sharing of payment data is something the majority of the respondents (65%) to the targeted consultation agree on. However, 45% of the respondents considered that the OB framework in PSD2 has not been successful, against 29% who found it successful (others were neutral). This is due to the various problems the respondents encounter, in particular as regards effective and efficient access of TPPs to data held by ASPSPs or the fact that despite the availability of APIs TPPs often continue to use the customer interface. The APIs can vary in quality and functionalities, causing too many OB operations to fail or providing a poor user journey. These problems are also emphasised in bilateral feedback from TPPs, through expert groups and also evidenced in the EBA Advice[53].

As described above, the current PSD2/RTS interface regime is very complex, with ASPSPs often having to facilitate access to data via two interfaces (API and fallback). TPPs regularly complain to the Commission and the EBA that the PSD2 APIs are inadequate and of low quality. According to TPPs, banks' APIs often do not return the information required, perform badly (e.g. returning many error codes and/or simply not being available), or banks block the TPP's access to accounts, despite the TPP acting on the basis of a PSU's consent. Furthermore, TPPs stressed that ASPSPs can take a long time to respond to a TPP's request for help, or their reporting of a bug, and even longer to resolve the issue. Some TPPs resort to using the fallback (i.e. the ASPSP's direct customer interface), to access the accounts, even though a PSD2-API is also available. This frustrates ASPSPs who do not observe high TPP traffic on their APIs created for PSD2 compliance purposes and still have to deal with a high request load on their direct customer interface[54]. This is illustrated by comparing the API calls by TPPs to UK banks[55] to the monthly website traffic/visits to the ASPSP's website. For example, the number of successful API calls to Barclays API was about 200 mln in November 2022, whereas the number of visits to the direct interface, Barclays.co.uk, was 9.7 mln. TPPs using the fallback interface increase the traffic a lot, which is a cause of concern to ASPSPs. It causes problems for TPPs which would prefer accessing data through APIs which is a superior and safer technology than direct access, and, when functioning, cheaper than the fall-back solution.[56] There is a visible trend of banks offering more and more APIs, also beyond or unrelated to PSD2. By March 2022, about half of the APIs offered were for PSD2 compliance (25%) and account reporting (23%), the other half covered other domains such as

[53] European Banking Authority (EBA/Op/2022/06) Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2), of 23 June 2022

[54] Han-Wei Liu: Two Decades of Laws and Practice Around Screen Scraping in the Common Law World and Its Open Banking Watershed Moment, 30(1) Washington International Law Journal, 2020; statistics on Open Banking API calls from the UK versus the number of visits to the respective banks websites shows that TPPs make many more API calls than that people visit the ASPSP's website (OBIE API data: API performance stats - Open Banking and website traffic: Free Website Traffic Checker & Analyzer | Website Rankings (semrush.com). There is no centralised data available on API calls for ASPSPs or TPPs in the EU.

[55] Data made available by the UK Open Banking Implementation Entity – such data does not exist in the EU.

[56] Information supplied in various responses by TPPs to the targeted consultation.

foreign exchange, investments, and digital identity, for which such interfaces are not (yet) a regulatory requirement [57].

ASPSPs report significant implementation costs for the development of APIs for OB[58] and the fact that the legislative framework provided in PSD2[59] and its RTS prevents ASPSPs from charging AISPs and PISPs for access to customer data and the relevant infrastructures that are in scope of PSD2[60]. This leads to OB being perceived as a pure regulatory burden (a mere compliance issue) by banks,[61] which claim that the free access does not incentivise them to offer the best possible API[62].

ASPSPs are also concerned and dissatisfied that some TPPs, acting as "API aggregator" pass on user data to unregulated "fourth parties"[63]. API aggregators specialise in developing interfaces with multiple ASPSP APIs, acting as intermediaries between ASPSPs and either licensed TPPs or unlicensed parties. This activity was not directly envisaged by PSD2. It emerged as a response to the multiplicity of bank APIs in the absence of an EU standard, but it can also be considered as a source of inefficiency in that it lengthens transaction chains and adds costs, as this 'API connection' service is not free to TPPs. Increasingly, one also sees AISPs that are not working directly for the end user (consumers, merchants etc) who gave them consent to access their data, but for "fourth parties" such as lenders wishing to evaluate creditworthiness, or companies wishing to provide a better service (e.g. an audit service) based on payment account data.[64] These fourth parties, not being licensed, are not allowed to obtain access to the account, but they receive the data from the licenced AISP. Although this is done with user's consent (GDPR consent for the unlicensed party and both GDPR and PSD2 consent for the licenced party), this "license as a service" model is quite different from the traditional AIS business model that was envisaged by PSD2[65], where a regulated party gathers and consolidates the payment account data and provides the AIS back to the end-user itself without other parties being involved. It is not however excluded by PSD2, as confirmed by the Commission in the EBA Q&A tool.[66]

---

[57] The Paypers, report 2022: The enablers of Open Banking, Open Finance, and Open Data; Innopay Open Banking Monitor, p. 8-10.
[58] See Annex 5 (Evaluation report); such one-off costs are reported by the ASPSP sector at over €2 billion.
[59] PSD2 requires that the provision of OB Services must not be dependent on any contractual relationship between PSPs and TPPs).
[60] As reported before, ASPSPs also provide non-PSD2 APIs to third parties for which they might charge a fee.
[61] See the evaluation at annex 5; such one-off costs are reported by the PSP section at about €2 billion, contrary to what was claimed in the 2013 impact assessment accompanying the Commission's proposal for PSD2, which assumed that "*the incremental cost related solely to the TPP access would be limited*".
[62] Responses to targeted consultation on respondents opinion of the success of Open Banking (question 33b), mostly from banks and/or banking associations.
[63] See the VVA/ CEPS study (pp.64-5) and also Annex 5 (sections 4.1.1. and 4.3.)
[64] Op cit, footnote 54 above.
[65] According to Open Banking Exchange, 14 TPPs provided such a service in 2022.
[66] EBA Q&A 2018_4098.

PSD2 and its implementing RTS chose not to impose an EU unique API standard (so as to not "counter the objective of promoting competition and innovation[67]"). Various market standards have nevertheless been developed. Stakeholders have spent resources and time on what should be provided via the dedicated interfaces (PSD2 APIs), what constitutes an obstacle to access etc. The situation has improved since EBA issued (non-binding) opinions on obstacles to OB[68], but problems of access and obstacles to Open Banking still remain and are regularly reported by TPPs to EU authorities.[69] Neither ASPSPs nor TPPs are fully satisfied with the current situation.

The drivers of the inefficiencies in OB are linked to the complexity of the legal framework (various interfaces, fallback obligation, possible fallback exemption etc.), to the lack of sufficient detail and clarity in the legislation about the expected performance level, the nature of the data, and functionalities to be made available to TPPs through OB interfaces, and to divergences in the framework's implementation and enforcement by the national competent authorities (NCA).

Regarding implementation of OB, it may be worthwhile to compare the EU to the UK, which for now still applies the same regulatory regime on OB deriving from PSD2. The UK has created a dedicated implementation body, the OB Implementation Entity (OBIE) and it has created and imposed a standardised API. As Annex 11 shows, the proportionate usage of OB and the variety of use cases is greater in the UK than in the EU, although there may be cultural factors at play also, the UK being therefore a more mature OB market. TPPs that are also active in the UK note that the implementation in the UK was less troublesome. However, it is not fully appropriate to make a direct comparison with the UK. The initial UK OB initiative had to deal with far fewer supervisors and ASPSPs, and no cross-border aspects. In the UK the OB process was driven by the Competition and Markets Authority (CMA), which, after an investigation into the UK's retail banking market concluded that competition within this market was insufficient and decided to require the 9 leading banks to find solutions together, through the OBIE. The UK underestimated the costs of implementing OB. An independent report to the CMA of October 2021 found that CMA originally estimated OB costs at £20 mln, which at the time of the report had already gone beyond £150 mln (nearly £19 mln per bank).[70]

2.1.3. Inconsistent powers and obligations of supervisors

The Commission's PSD2 review presented in the Evaluation Report (Annex 5) has revealed inconsistent application and insufficient enforcement of PSD2 provisions and found that many of the limitations to progress on PSD2's objectives link to challenges related to varying powers and obligations of supervisors. Inconsistent application of the legal framework and insufficiently robust enforcement of rights and duties was often mentioned in stakeholders'

---

[67] European Banking Authority (EBA/OP/2020/10) Opinion of the European Banking Authority on obstacles under Article 32(3) of the RTS on SCA and CSC; and (EBA/Op/2021/02) Opinion of the European Banking Authority on supervisory actions to ensure the removal of obstacles to account access under PSD2.
[68] See EBA Opinions referred to in previous footnote.
[69] See for example : European Third Party Providers Association - PSD2 Obstacles (etppa.org)
[70] Investigation of Open Banking Limited by Alison White, available here.

constributions on various topics, as well as noted by the EBA in its Advice. Specific examples in each area, enforcement and implementation, are given below.

- *Enforcement insufficiencies*

PSD2 currently contains only high-level rules regarding penalties, leaving discretion at national level to decide what kind of rules to be introduced for breaches of PSD2 provisions (including rules on the publication of an infringement) and how these rules will be applied. Whereas the application of penalties is currently governed by national administrative law provisions, this has resulted in diverse and often lengthy processes in each Member State. Relatively few PSD2 related penalties for OB breaches have been imposed by national competent authorities.

Slow or ineffective enforcement has often been brought up in the targeted consultation as a key factor linked to stakeholders' general views that PSD2 provisions on OB have not been successful (only 29% of respondents find the framework has been successful, against 45% that find it has not). Regarding issues related to the implementation of data access interfaces in Open Banking, many TPPs stressed the ineffective enforcement by regulators.[71] EBA in its Advice highlights a number of challenges reportedly faced by national supervisors in relation to enforcement. These include the significant time, resources and specific skills needed to supervise technical specifications of innovative IT systems and solutions.

Certain consumer rules in PSD2 are barely enforced due to the lack of any designated competent authority; this is the case for example as regards independent ATM operators, which are not subjected to ongoing supervision, but which must apply transparency on pricing. Users have drawn attention to unpunished breaches of PSD2 in this area.[72]

- *Divergences in application*

The evaluation has identified differences between national authorities in licensing requirements, the duration of the application process, and regulatory requirements of operating across borders. Besides making such activities more difficult, one effect is to introduce scope for regulatory arbitrage, as entities can passport their services across Europe after having established themselves in one Member State where licensing and supervisory practices might be deemed more favorable. With regard to opening and maintaining a payment account, some Member States impose higher requirements than others. Furthermore, PSD2 allows alternative methods of calculating the own funds requirement for Payment Institutions. Findings from the targeted consultation, as well as the EBA Advice, point to divergences between Member States in determining who is responsible for choosing the method for the calculation of own funds; in some cases PIs have been allowed to choose the method themselves, in others not.

One limitation to the success of the PSD2 framework on passporting notifications for agents and distributors has been the divergence in practices amongst NCAs in assessing whether cross-border activities carried out by licensed entities using agents or distributors fall under the right of establishment or the freedom to provide services.

---

[71] See for example:, ETPPA Position Paper on PSD2 review, June 2022; or OFA position paper on PSD2.
[72] See for example BEUX-X-2022-118_BEUC_position_paper_on_PSD2_review.pdf p.5

An example of divergent implementation in the area of Open Banking is a lack of consistency in how the definition of "payment account" is interpreted across the EU. There is uncertainty in the market as to whether certain types of accounts, such as electronic money accounts linked to prepaid cards, savings accounts, reference accounts, credit card accounts and others, should be considered payment accounts. This has led to uncertainty regarding the different types of account data which can be accessed by AISPs and PISPs across the EU, with, for instance, AISPs being able to access credit card data in some jurisdictions but not in others.[73]

Another case where divergent interpretation and application of provisions across Member States create opportunities for regulatory arbitrage concerns the list of exclusions, in particular the so-called 'limited network exclusion' under Article 3(k) of PSD2. Here the EBA has noted how the application of the requirements to fall under this exclusion have diverged significantly between Member States, which led the EBA to adopt Guidelines on this exemption.[74]

2.1.4. Unlevel playing field between banks and non-bank PSPs

The issue of interaction between PSD2 and the Settlement Finality Directive (SFD), with the consequence of preventing direct access of non-bank PSPs to certain key payment systems, is highlighted in the Evaluation Report. The SFD lists the participants that are allowed to participate directly in systems designated by Member States pursuant to the SFD[75], but Payment Institutions and E-Money Institutions do not appear on the list.

The SFD protects a duly designated, notified and published system and its participants from the legal uncertainty and unpredictability inherent in the opening of insolvency proceedings against one of their participants. It does so by stipulating the irrevocability and finality of transfer orders entered into an SFD system, thus preventing them from being interfered with in such proceedings (settlement finality). It also provides for the enforceability of the netting of transfer orders, from the effects of the insolvency of a participant. Moreover, the SFD ring-fences collateral security provided either in connection with participation in an SFD system or in the monetary operations of the Member States' central banks or the European Central Bank (ECB) from the effects of the insolvency of the collateral provider. SFD leaves to Member States the decision whether or not to designate and notify a system governed by the laws of that Member State; a large number of payment systems have been designated by various Member States under SFD, including EU-wide systems operated by the ECB and the ESCB, such as TARGET2 or TIPS.[76]

PSD2 currently does not contain any supervision or licencing regime for operators of payment systems[77], and only article 35 contains high-level rules applicable to payment system operators. This article requires that the internal rules of payment systems, including

---

[73] See EBA Advice p.12.

[74] Article 3(k) excludes from PSD2 scope, with conditions "services based on specific payment instruments that can be used only in a limited way". See European Banking Authority (EBA/GL/2022/02), Guidelines on the limited network exclusion under PSD2, 24 February 2022

[75] Article 2(f) SFD.

[76] The full list of SFD-designated systems is available from the European Securities and Markets Authority, here.

[77] See Annex 6 on the question of whether such operators should be brought within the scope of PSD2.

access rules, must be Proportional, Objective and Non-Discriminatory (the "POND" principle). However, payment systems designated under SFD are excluded from this requirement under article 35.2(a). This exclusion was already in PSD1 of 2007 and was not changed or removed with PSD2.

PIs and EMIs may alternatively access SFD-designated payment systems "indirectly" via an account held with a bank. Access to a commercial bank account is also essential to allow non-bank PSPs to safeguard customer funds, without which they also cannot provide payment services. In this context, it can be noted that Article 36 of PSD2 requires a bank to notify its competent authority, in writing and with explanation, where it refuses to grant an applicant non-bank PSP access to a bank account. However, article 36 of PSD2 does not require any notification or explanation in cases when the bank closes the PI or EMI account. This allows banks to grant PIs and EMIs access to a bank account but to subsequently withdraw that access with no consequences. In such cases, the non-bank PSP is also exposed to withdrawal of service by the bank, which is usually justified by a pretext of "de-risking" (for example on AML grounds).[78] A number of PIs and EMIs have informed the Commission that they are regularly "offboarded" by banks with only perfunctory or no explanation, thus causing interruption of service until a replacement commercial bank is found, requiring burdensome transferral of connectivity of their infrastructure to the new bank. Thus, even indirect access to key payment systems is uncertain, and there is a risk of periods with no access at all to payment systems and no ability to safeguard customer funds, both of which are essential for a PI or EMI to carry out its core business.

2.2. What are the consequences of the problems?

The consequences of the problems should be considered for each category of stakeholder: payment system users, PSPs, Open Banking providers (TPPs), and single market and macroeconomic consequences.

Users (both consumers and businesses, including merchants) may suffer detriment and lose confidence in payment services. Firstly, fraud is still seen by a significant number of users as a major threat to their trust in digital payments. The results of the open public consultation on the PSD2 review show that 17% of the respondents (11 out of 66) indicate they have been the victim of fraud recently. Out of those 11, 4 requested a refund with their payment service provider and received it in full. Three out of those 11 respondents filed a request but did not receive a refund.

A second consequence for users is that prices of payment services may be higher than necessary due to hindered competition. For example, the problems encountered by PIs and EMIs to offer payment account services in competition with banks reduces the competitive pressure on banks and can inhibit price competition between different categories of PSPs. Also, the lack of clarity regarding agents and distributors noted above creates difficulties for consumers in identifying the applicable consumer protection measures and the relevant authority for specific supervisory purposes and complaints handling.

[78] European Banking Authority (EBA/Op/2022/01), Opinion of the EBA on 'de-risking', January 2022.

The large potential savings for payees, particularly merchants, from PIS payments replacing more costly means of payment such as cards, anticipated in the impact assessment accompanying the PSD2 proposal in 2013, have largely not been realised. The inefficiencies in the functioning of Open Banking (OB) in the EU identified above limit the supply and usage of OB services and increase their cost, also hindering the development of innovative cost-saving services based on OB. The relatively low take-up of OB services in the EU described in Annex 11, despite the high numbers of TPPs created both before and after PSD2 (around 500), may well be linked to these factors, although causality is difficult to establish.

For PSPs, the consequences include uncertainty about their obligations due to lack of clarity in places in the legislation. The problems regarding divergent implementation and enforcement of PSD2 directly impact competition between PSPs, by creating different regulatory conditions in different Member States through different interpretation of PSD2 rules, encouraging regulatory arbitrage. Indeed, as evidenced in the VVA/CEPS study,[79] there is a concentration of licensing of payment fintechs (TPPs) in a number of relatively smaller Member States from which services are performed largely on a cross-border basis. The imbalances in numbers of TPPs across Member States can be seen in Figure 5 below. PSPs based in Member States with stricter interpretations of PSD2 rules face cross-border competition from PSPs based in Member States with 'less strict' interpretations/licensing regimes. PSPs, especially those which are OB TPPs, often report that complaints against other PSPs (for example for denial of access to user data with user consent) are not followed up, thus limiting their ability to provide OB services.

Figure 5[80]

	Euro (from 579 to 987)																			Non-Euro (from 303 to 371)							
	BE	DE	EE	IE	GR	ES	FR	IT	CY	LU	LV	MT	NL	AT	PT	SI	SK	FI	LT	BG	HR	CZ	DK	HU	PL	RO	SE
2014	29	53	10	14	13	75	44	73	14	18	48	24	36	12	46	5	13	12	40	11	7	123	n/a	18	33	14	97
2022	33	103	19	47	24	94	84	73	28	29	17	48	151	19	28	8	19	21	142	17	12	113	28	27	48	15	111

The impediments to access to payment systems for non-bank PSPs harm competition and innovation, by preventing non-bank PSPs from developing and offering payment services in competition with banks, for example instant payments, resulting in higher prices for consumers and less innovative payment services. The fact that, in order to connect to SFD-designated payment systems in the EU, non-bank PSPs must use an indirect connection offered by a bank or another SFD eligible participant as a commercial service, creates a dependency on banks. In addition, as non-bank PSPs are competitors to banks, and due to the access dependency, the banks might gain insight to the non-bank PSP's confidential business information, which might raise concerns from a competition point of view. Furthermore, the service is charged by the bank to the PI or EMI, thus involving an additional cost and impacting their competitiveness on the payments market[81]. There is thus a level playing field issue, in so far as certain categories of participants in the payments market are dependent on their competitors in order to offer a basic payment service.

[79] Page 33 and ff.
[80] ECB data, available at this link: . Reproduced in the VVA/CEPS study p.33.
[81] However, in this case the intermediary bank, not the PIs and EMIs, must fulfil potential collateral requirements of the payment systems, thus to some extent justifying the charges.

Open Banking TPPs may experience difficulties in providing their basic services due to inadequate OB interfaces and lose business as a result.

As for macroeconomic consequences, given the importance of payments for economic activity, any unnecessarily high cost or inefficiencies in payment instruments will inevitably dampen and slow down transactions, with consequences for GDP.

Regarding the single market, insufficiencies and inconsistencies in enforcement and implementation produce different operating conditions in different parts of the single market, causing legal uncertainty, fragmentation and distortions. For example, a large number of PIs and EMIs are authorised in certain smaller Member States and provide services cross-border throughout the EU. PSPs in other member States suggest that these PIs and EMIs benefit from more generous interpretations of certain PSD2 rules.

2.3. How likely is the problem to persist?

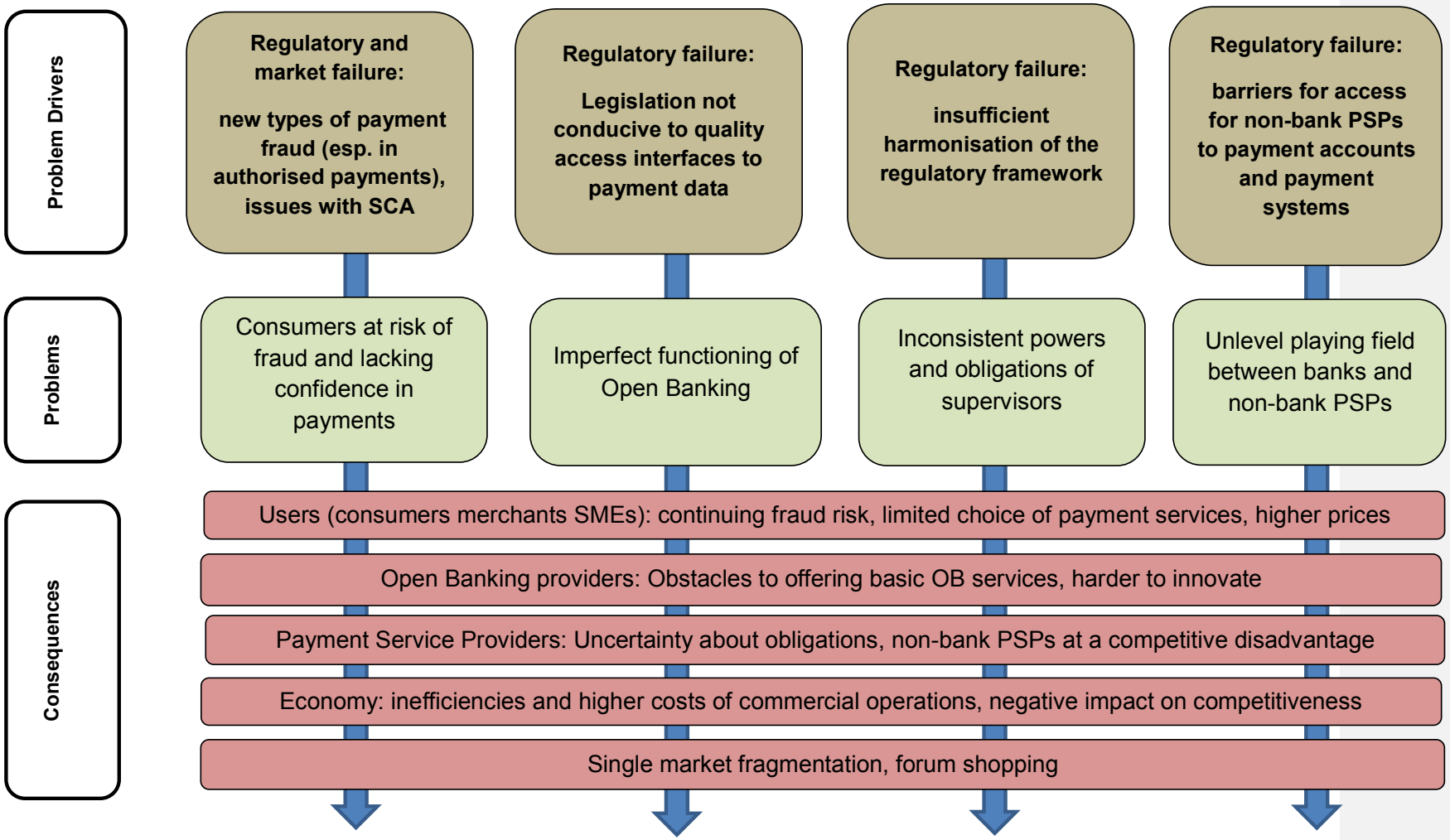
Fraud is in constant development, with fraudsters always adapting to new legal frameworks and operating environments and finding new techniques of fraud. Fraud will always exist, but it can be reduced in scale and its impacts mitigated by appropriate regulatory frameworks. As long as the legislation containing the identified issues remains in force, certain useful anti-fraud actions by PSPs will be hindered or prevented.

Regarding Open Banking, the problems could be mitigated to a certain extent by more vigorous enforcement. If not revised, the PSD2's complex and costly regime (e.g. on interfaces, dedicated interface fall-back, exemption to fall-back etc.) and the large variations in what data can be accessed by TPPs under EU regulated OB rules will remain and the success of OB will therefore remain limited.

The identified problems which are regulatory in origin, including gaps and ambiguities in the rules, will persist in absence of amendment of the legislation in question. This applies for example to the issues identified in section 2.1.3 above and also to the issue of direct access of PIs and EMIs to payment settlement systems designated under SFD.

Section 5.1 (baseline scenario) provides a more detailed description of the expected evolution in the case of no new policy initiative by the European Union.

2.4. Problem Tree



3. WHY SHOULD THE EU ACT?

3.1. Legal basis

The current legal basis of the PSD2 Directive is Article 114 of the Treaty on the Functioning of the European Union (TFEU), the single market article, due to the importance of establishing a true single market for payments in the EU. It follows that any amendments to PSD2, either in a new Directive or a Regulation, should also be based on this Article. Article 114 is also the legal basis of the Settlement Finality Directive. The Directive on E-Money Institutions[82] is based on articles 53 and 114, and it follows that any new legal act incorporating rules for authorisation of EMIs (see §7.8 and Annex 8) should follow such a dual legal base.

3.2. Subsidiarity: Necessity of EU action

As this is a review and revision of existing EU secondary law, this can only be done at EU level, taking into account the objectives of PSD2 to create a competitive and innovative single market for payments while protecting payment service users and ensuring security and ease of payments. The importance of performing this review at EU level is also highlighted in the Commission's 2020 Retail Payments Strategy.[83] The strategy not only highlighted the strategic importance of a vision for European retail payments, but also concluded that the EU payments market remains fragmented along national borders, despite recent improvements. This fragmentation across the EU may hinder further innovation, and thus pose a risk to achieving the objectives of the Directive.

3.3. Subsidiarity: Added value of EU action

The demand for cross-border payment activities has always been a key factor justifying EU legislation in the field of payments, both as regards cross-border payments, and cross-border provision of payment services in the single market. Companies are actively making use of both passporting and establishment in different national jurisdictions. Payment service users (including consumers) are also making more use of cross-border service providers. Member States may take divergent approaches to supervise and enforce PSD2, which leads to entities active in different Member States being subject to different requirements for similar functionalities and/or services. This issue is best addressed at EU level to ensure more consistent supervision and enforcement of PSD2. Aligning EU rules further, taking into account recent developments in the payments market, would also support the further integration of an internal market for payment services.

---

[82] Directive 2009/110/EC of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of E-Money Institutions.
[83] See footnote 27 above.

4. OBJECTIVES: WHAT IS TO BE ACHIEVED?

4.1. General objectives

As a reminder, there were five general objectives of PSD2, as expressed in the impact assessment of 2013 accompanying the Commission's proposal for PSD2:

1. To ensure a level playing field between incumbent and new providers of card, internet and mobile payments;
2. To increase the efficiency, transparency and choice of payment instruments for payment service users (consumers and merchants);
3. To facilitate the provision of card, internet and mobile payment services across borders within the EU by ensuring a Single Market for payments;
4. To create an environment which helps innovative payment services to reach a broader market;
5. To ensure a high level of protection for PSUs across all Member States of the EU.

The evaluation (Annex 5) finds each of these general objectives to have been partially achieved, some to a greater degree than others.

4.2. Specific objectives

The specific objectives correspond to the elimination or mitigation of the identified problems, and are therefore four in number:

1. Strengthen user rights and protection against fraud (relating to general objective 5)
2. Improve the competitiveness of Open Banking services (relating to general objective 4)
3. Improve enforcement and implementation in Member States (relating to general objective 3)
4. Improve (direct or indirect) access to payment systems and bank accounts for non-bank PSPs (relating to general objective 1).

Measures to clarify the scope of PSD2, other technical clarifications, and the integration of EMD2 into PSD2, covered in Annexes 6-9, are related to general objective 3 (Single Market). Measures to improve access to cash in Annex 9 are related to general objective 5 (protection of payment system users). Consumer rights measures, related to general objective 2 (efficiency, transparency and choice) and 5 (protection of payment system users), are covered in Annex 10[84].

[84] Under general objective 2, PSD2 has a specific objective « to address standardisation and interoperability gaps for card, internet and mobile payments », which is found in the evaluation report to be not achieved. However, the objective of interoperability is now being pursued essentially via the SEPA Regulation (for payments in euro) and the Commission's legislative initiative of 2022 on instant payments is an example of this.

5. WHAT ARE THE AVAILABLE POLICY OPTIONS?

5.1. What is the baseline from which options are assessed?

In the baseline scenario the EU rules on payment services covered by PSD2 would remain as they are with no modifications (other than those stemming from other present or future EU initiatives having an impact on PSD2 such as DORA, instant payments, the Data Act or the future Open Finance or Digital euro framework). It should be emphasised that the evaluation (see Annex 5) has found that the EU payments market functions better now than before PSD2. There are more providers of payment services than before PSD2, including innovative fintechs, and a wider range of services is available, including on a cross-border basis. However, the PSD2 objectives concerning the EU payment market remain only partially achieved.

Regarding user protection against fraud, SCA would remain applicable with the current uncertainty about and misuse of certain exclusions from its scope (e.g. MOTOs and MITs), and PSP liability would continue to be limited to fraud concerning unauthorised transactions. Uncertainty would remain in certain cases as to which actor in a payment chain is responsible for performing SCA. IBAN/name verification will be required for instant payments only (based on the Commission's proposal on instant payments – see Annex 12), not for non-instant credit transfers.

As regards Open Banking, the baseline would involve TPPs having continued free access to account data via interfaces provided by ASPSPs, either a dedicated interface solely for the purpose of PSD2, or via direct access to the interface the ASPSP uses to communicate with its customer as well (customer interface). Variations would continue as to what data TPPs can access. Provision of a fallback means of access to account data in case of API failure (heavily criticised by banks as a major source of costs, due to the need to maintain two OB compliant interfaces) would remain obligatory, with its complex, costly and resource-intensive (for both ASPSPs and supervisors granting the exemption) fallback exemption corollary. For TPPs, access to account data would remain free of charge as regards the data to which access is required by PSD2 and its RTS, but uncertainty would remain as to what the PSD2 free "mandatory" data is. The distinction between baseline and added-value services would remain unclear (as in PSD2), causing inefficiency for Open Banking itself, but also uncertainties for the outcome and workability of market driven OB initiatives[85], which depend on a clear delineation between what is a PSD2 "mandatory" service and what is 'value-added'. Nevertheless, private sector forecasts are for continuing growth in numbers of OB users, even on the baseline scenario.

The proposal for a Data Act, currently in discussion in the European Parliament and the Council should also be considered as part of the baseline. The Data Act Chapter III establishes obligations in business-to-business data sharing applicable to data holders legally

[85] Such as the SPAA initiative of the European Payments Council, an initiative to develop a "scheme" for payments data to which there is no mandatory access under PSD2. See The SEPA Payment Account Access (SPAA) Scheme Rulebook

required to make data available. The compensation rules under Chapter III of the Data Act would not apply in the baseline/no action scenario, as the Data Act "grandfathers" existing data access compensation regimes such as the Open Banking rules of PSD2. Payment data falling outside the scope of PSD2 rules (i.e. those not available to the PSU through the consumer banking interface) would not be subject to the Data Act, as the Data Act only applies where there is mandatory access to data.

As regards the divergences in interpretation and implementation including enforcement, the baseline scenario would amount to continuing with the existing EU rules on payment services as transposed by Member States but with their unclarities, and as interpreted and enforced often divergently by NCAs. Member States' rules on penalties applicable to infringements of the national law transposing PSD2 would remain very different. The Commission would only be able to provide interpretative non-binding guidance, for example in the framework of questions raised by market actors via the Question-and-Answer tool provided by the EBA.[86] Supervision would be basically along national lines with national competent authorities responsible within their jurisdictions, although some rules on cooperation among national competent authorities (in case of cross-border services) including on exchange of information, would continue to exist. There would continue to be an uneven playing field with potential for regulatory arbitrage, with PSPs choosing those Member States that practise the application of EU rules on payment services that is advantageous for them and carrying out cross-border services in other Member States which apply different rules to PSPs established there.

As regards access to payment infrastructure, the baseline would involve non-bank PSPs lacking direct access to key payment infrastructures and remaining dependent on banks for access, involving higher cost, risk of withdrawal of service, and the possibility of banks gaining insight to their confidential business information. Banks would remain obliged to justify to competent authorities any refusal to provide account services to non-bank PSPs, but would remain able to provide brief "pro forma" justifications, and would also not be obliged to explain any withdrawal of service to PIs and EMIs (account closure). The negative effects on competition between PSPs, described above, would thus remain.

5.2. Description of the policy options

It should be noted that the options are largely independent and not inter-related, although the options to improve enforcement and implementation in Member States can reinforce and contribute to all the other objectives.

5.2.1. *Strengthen user rights and protection against fraud*

Other than the baseline, four options are considered in the area of fraud reduction, which are mutually compatible, with the exception of 1.d) and 1.e) which are mutually exclusive:

1.a) Measures to improve the application of SCA

[86] European Banking Authority, List of Q&As

In order to reduce improper use of the MOTO and MIT exemptions, this option first includes the introduction of clear definitions of MOTOs and MITs and clarification on the general treatment of these transactions in light of existing guidance[87]. In respect of MITs, this would involve the need to apply SCA at the set-up of the mandate (because this action is payer initiated), without the need to apply SCA for subsequent (merchant-initiated) payment transactions. There would be clarification of the regulatory approach to MITs in general and direct debits specifically aligning the applicable legal requirements to both transactions, which would logically mean applying the same consumer protection measures, such as refunds, to direct debits and MITs as being both transactions initiated by the payee within the meaning of article 76 PSD2.[88] In respect of MOTOs, since there is currently no definition in PSD2 (only a mention in recital 95), one would be added, along with provisions on the general treatment of MOTOs. In particular, legal clarity will be provided that transactions whose 'initiation' is non-digital are excluded from the SCA obligations even if the subsequent 'execution' is digital. Currently there is uncertainty as to whether both the initiation *and* the execution should be non-digital in order for SCA not to apply.

1.b) Legal basis for PSPs to share information on fraud and obligation to educate customers about fraud

This option packages two components which, although not inherently related to each other, both concern anti-fraud actions by PSPs. They are therefore presented as a single option for simplicity.

There would be a provision allowing PSPs to share payment fraud data with each other to the extent necessary to comply with the legal obligation for PSPs to have transaction monitoring mechanisms (TMMs)[89] in place (as detailed in Annex 7 on technical clarifications and other changes). It would provide for lawfulness for such processing activity under the GDPR without creating an obligation for PSPs to share payment fraud data.

There would also be an obligation on PSPs to carry out customer 'education' and awareness programmes on fraud risks, with the aim of enhancing consumer awareness and education about fraud (especially the new types of fraud) and the risks of certain payment instruments/methods. Specific requirements would be introduced in the legislation on educational and awareness programs for fraud risks (also addressed towards employees of

[87] As detailed in the problem definition section above, for MITs, through the EBA's EBA Q&As 2018_4031, 2018_4131, 2018_4404, 2019_4791, 2019_4792, 2019_4794 on the Applicability of SCA to 'card payments initiated by the payee only'. For MOTOs, Q&As 4058, 4790, and 4788, respectively on transactions initiated via Interactive Voice Response solutions, keyed Mail Order or Telephone Order transactions and treatment of electronic bookings similar to Mail Order and Telephone Orders transactions.

[88] As proposed by the EBA, in its Advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2), 23 June 2022, page 76.

[89] Under Article 2(1) of the RTS, PSPs must have TMMs in place that enable them to detect unauthorised or fraudulent payment transactions for the purpose of applying SCA or exempting them from applying SCA, subject to specified and limited conditions laid down in Article 18 of the RTS.

PSPs), as proposed by EBA[90], building on the EBA Guidelines on ICT and security risk management.[91] In line with those EBA Guidelines, there would not be detailed prescriptive requirements, given the risk that such requirements would quickly become obsolete due to the ever-changing nature of fraud-related risks.

1.c) Extension of the requirement to provide IBAN/name verification by PSPs from instant payments to all credit transfers

Verification of concordance between the name of a payee and the bank account number (in IBAN format) is a service already provided domestically for example in the Netherlands[92] (and in the UK where it is called Confirmation of Payee[93]), which ensures that before they authorise a payment, payers are informed of the degree of 'match' between the name and IBAN of the payee. The payer decides, based on the feedback received (divergence or close concordance; in case of total concordance there is normally no notification), whether to proceed with the credit transfer. The Commission's legislative proposal on instant payments (IPs) requires PSPs offering IPs to offer this service to their users[94]. This option would extend that requirement from instant credit transfers in euro to all credit transfers, instant or not, in euro or other EU currencies. As in the proposal on instant payments, the service would be optional for the PSU and could be subject to a fee.

1.d) Full reversal of liability between users and PSPs for fraudulent authorised transactions

This option would introduce a refund right for PSUs in cases where a transaction was the result of fraud, even if the user authorised the transaction via SCA (APP fraud, as discussed in section 2.1.1.). Today such a refund right only exists for 'unauthorized' transactions under PSD2 (article 73 and 74), commonly understood (in the absence of a definition) as transactions where the payer could not have authorised the transaction via SCA as, for example, his card was stolen – unless there is for example gross negligence of the payer. This would be a significant departure from the current regime which only provides a refund right in case of unauthorised transactions. The objective of this option would be to motivate and incentivise PSPs, through their full financial liability if fraud does occur (both in unauthorised and authorised transactions scenarios), to undertake more effective anti-fraud initiatives, thus contributing to an overall reduction in fraud.

---

[90] European Banking Authority (EBA/Op/2022/06) Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2), of 23 June 2022, page 82.
[91] The EBA Guidelines on ICT and security risk management (EBA/GL/2019/04), which could serve as a model for the educational and awareness programs for fraud risks.
[92] See SurePay - We're here to make online payments safer
[93] See Confirmation of Payee - Pay.UK (wearepay.uk)
[94] Proposal for a Regulation amending Regulations (EU) No 260/2012 and (EU) 2021/1230 as regards instant credit transfers in euro (COM(2022) 546 final). See Annex 12. The IBAN verification service is discussed at length in the impact assessment accompanying that proposal (SWD(2022) 546 final).

1.e) Conditional reversal of liability between PSUs and PSPs for fraudulent authorised transactions

This option 1e presupposes the selection of option 1c) on IBAN/name verification. Unlike the full liability reversal described under option 1.d), this alternative option would introduce limited changes to the liability regime between PSUs and PSPs for fraudulent authorised transactions. This would be done by the introduction of a refund right for consumers who are victims of APP fraud, but limited to cases where the payment service provider of the payer failed to notify the payer of a detected discrepancy between the unique identifier and the name of the payee provided by the payer.. In such a case the PSP(s) that did not apply the necessary preventive measures (payer and/or payee PSP) would bear liability if it turns out to be a fraudulent payment, even if it was authorised by the payer through SCA. The payer's PSP would refund the payer, and could itself claim compensation from the payee's PSP, if that PSP were at fault (for example, not responding to an enquiry regarding IBAN/name correspondence of the payee). Furthermore, this option would grant consumers (except in cases of gross negligence or where the consumer is himself the fraudster) a refund right when they were manipulated by a third party pretending to be an employee of the consumer's payment service provider using lies or deception such as the bank's name and/or telephone number and this manipulation gave rise to subsequent fraudulent authorised payment transactions under the condition that the consumer has, without any delay, reported the fraud to the police and notified its payment service provider.

5.2.2. Improve the competitiveness of Open Banking services

Other than the baseline, four options are considered. Most of the options can be combined with any other, but options 2c) and 2d) are alternatives.

2.a) Requirement for a dedicated data access interface

This option would impose on ASPSPs an obligation to make available to TPPs a dedicated Open Banking interface for the purpose of data access[95], instead of keeping the current choice for ASPSPs between providing either a dedicated interface or an adapted customer-facing interface. This would mean that TPPs must only access data through this dedicated interface, and would no longer have the right to access the data 'directly' through the customer-facing interface, as many TPPs often do today even when a dedicated interface (usually an API) is made available to them. There would no longer be a requirement for ASPSPs offering an API to also maintain another interface (as a 'fallback' interface); consequently, the current possibility of an ASPSP obtaining a fallback exemption from a supervisor, allowing it to maintain only one interface[96], would become redundant. Exemptions from the requirement to

[95] A carve out can be applied for specific ASPSPs, for example for those that do not service retail customers, or are active in a niche market with little to no TPP activity/demand for access to the payment accounts they hold. These ASPSPs would still be allowed to provide a PSD2 interface, but this would be voluntary.

[96] This was the original plan for PSD2 as well, but due to concerns from the TPP sector about the ASPSPs readiness to provide adequate APIs, who feared business continuity issues, ASPSPs were required to *also* offer the fallback, even if they built a dedicated API. To mitigate a multitude of interfaces, ASPSPs obtained the right to request a fallback exemption from their NCA.

provide a dedicated interface could be considered for cases where it may be disproportionate to require the ASPSP to offer a dedicated interface. In this respect, EBA would be mandated to develop a set of criteria for granting such exemptions.

2.b) Permission dashboards

This option would involve the implementation of an Open Banking permissions 'dashboard', to help data owners have an overview of and easily manage the data access permissions that they have given to TPPs. The new OB permissions dashboard would be required to provide an overview of outstanding AIS and PIS permissions, including basic information such as the purpose and duration of the permission, and would allow the account holder to block payment account data access to a given TPP. The ASPSP would be obliged to inform the concerned TPP without undue delay if a data access permission is withdrawn.

2.c) Impose a single, harmonised, API standard for TPP access to account data

This option would fully harmonise the current interfaces through the imposition of a single, EU-wide API standard. This standard would replace the existing market standards that exist in the EU ('STET' standard, 'Berlin Group' standard etc.), as well as the many individual bank declinations of these various market standards, and the APIs that banks have built without reference to any market standard. The standard would cover operational rules and implementation guidance including required data formats and technical specifications, and would also describe the use cases that are covered by the standard (e.g. single payment initiation, obtaining an account's transaction history etc.). The API standard would need to be designed by industry and imposed by delegated legislation; it could be one of the existing standards or a new one. Stakeholders would have to adjust where necessary their existing APIs to implement this new API standard. As a whole, the standard would comprise everything which is required to be compliant with the rules on data access. Being a mandatory and 'full' standard, this option would leave no room for individual differences in the OB APIs.

2.d) Specify in more detail minimum requirements for OB data interfaces

This option would make certain amendments and clarifications to the rules on access to payment account data and also move some of the specifications currently in the RTS to the Regulation. Currently the payment data to which access is mandated in PSD2 is the same data as that which the customer can access via the customer interface ("parity principle"[97]) and thus varies from PSP to PSP and has sometimes led to disagreement between ASPSPs and TPPs as to which data was made to be available via the OB API and which not. It was not seriously considered to mandate access to all payment data of a user which a PSP might possibly hold, as this would have been a disproportionate open-ended requirement. It was not considered to remove the parity principle either, because the customer already has access to

[97] The information and functionalities within scope of PSD2 that are available to PSUs in the direct customer interface of their ASPSP is expected to also be made available if the PSU accesses its account via a TPP (RTS on SCA and CSC, art. 36(1)(a)).

this data in the direct customer interface, and it would be a step back from what is currently required to be made available by ASPSPs. This option thus upholds the parity principle; the minimum requirements are not intended to narrow down the parity principle, but they will create a baseline that will be the same across all ASPSPs and provide a comparable minimum workable solution for TPPs. This option will in particular create clarity for Payment Initiation Services and the types of payment services they will be able to provide via the ASPSP's OB APIs, and it will also clarify some of the data elements that AIS providers should be able to access (but only basic data like the name of the account holder, which is not always available under the parity principle, as not all customer interfaces show the customer's own name).

What is made available via the OB interfaces could still vary between PSPs, as the parity principle can give different outcomes from ASPSP to ASPSP depending on what they make available in their customer facing interface, going beyond the minimum. The minimum requirements would include core elements which are considered to be indispensable to ensure a satisfactory OB journey, both in terms of data and what can be done with that data ("functionalities"). The option would thus define an absolute minimum to the OB API and provide more detail than the requirements currently contained in PSD and the RTS. The minimum requirements would be built on what is already in the RTS[98], and be extracted from sources such as the EBA Advice, and TPPs' input[99]. They would consist of data to be made available, payment services to be supported and the availability and performance of the interface. To limit the burden on ASPSPs, the number of these functionalities and data points would be kept limited[100]. The key such mandatory data points and services would be:

- the payee's name and IBAN (not always included in customer interfaces);
- PISP-specific services, such as a confirmation from the ASPSP that the payment will be executed, status of the payment, allow the PSU to set up and stop a standing order or a future dated payment through a PISP.

2.e) *abandon the non-contractual/no charging default approach*

This is the most radical option for Open Banking, as it would involve reversing one of the key principles of OB under PSD2, that access to the required payment data must be possible free of charge for TPPs. This principle is not stated explicitly in PSD2, but is implicit in the legal requirement in PSD2 that data access must not be conditioned on the existence of a contract between the parties (ASPSP and TPP), since any payment of fees necessarily requires a contractual relationship. This option would allow ASPSPs to require a contract and

[98] Such as RTS art. 32 (which includes availability and performance) and 36 (which includes data parity)

[99] For example: European Third-Party Providers Association, ETPPA Position Paper on PSD2 review, June 2022; Open Finance Association, OFA position on the review of the Revised Payment Services Directive (PSD2), September 2022.

[100] As the OB APIs of the ASPSP (largely) depend on what is already in the customer-facing interface, any minimum requirements an ASPSP might have to make available in the OB API, which is currently not available in their customer interface might lead to such ASPSP putting in additional resources compared to ASPSPs who already have all these minimum requirements included in their customer-facing interface as well.

payment of a fee as a condition for access to payment account data by a TPP. The purpose of this option would be to respond to the argument often given (by banks) for low-quality APIs that the ASPSPs were not compensated for their expenses to design data access infrastructures and therefore had no motivation to invest in high quality interfaces.

5.2.3. Improve enforcement and implementation in Member States

Other than the baseline, three mutually compatible options are considered:

3.a) Replace the greater part of PSD2 with a directly applicable Regulation

In this option EU rules on payment services would be harmonised in more detail by incorporating more detailed rules in a directly applicable Regulation. The set of rules would be restructured to reduce and minimise Member States' margins of interpretation and ability to add further rules. This further harmonisation would involve placing rules concerning payments in PSD2 in a Regulation in particular, those provisions of PSD2 addressed to individual payment services users and their relationship to PSPs or the rights and obligations of AISPs and PISPs. Only provisions on licensing and supervision of Payment Institutions, corresponding to Title II of PSD2 (and on licensing and supervision of E-Money Institutions, corresponding to the current Electronic Money Directive – See Annex 8) would remain in the form of a Directive.[101] This option would also involve a higher level of harmonisation in EU payments rules via reduction of ambiguity and lack of clarity, and an addition of greater detail. Numerous areas would benefit from clarifications and specifications, amongst others the list of definitions and exclusions, licensing and supervisory requirements and others. These adjustments would be based on inter alia replies provided by the European Banking Authority in the context of the Question-and-Answer tool. See Annex 7 for details of clarifications to be provided (Annex 6 for clarifications on scope)[102].

3.b) Strengthen provisions on penalties in PSD

This option involves measures to allow for improved and more harmonised powers regarding penalties in case the rules are breached. There would be a list of provisions for which National Competent Authorities must have sufficient sanctioning powers (for instance, in the areas of SCA application, Open Banking access to accounts, or bank account services for PIs and EMIs), accompanied by criteria on the level of penalties; however, levels of penalties such as fines to be imposed by Member States for specific breaches would not be fully harmonised. The power of EBA to temporarily prohibit certain products in case of risk to consumers would be operationalised in the area of payments[103].

---

[101] See Annex 8 on the envisaged integration of EMD into PSD and annex 7 amongst others on the envisaged technical amendments to the provisions on licensing and supervision of PIs.

[102] The clarifications outlined in Annexes 6 and 7 could be implemented either via a Regulation or via a Directive.

[103] The broad « product intervention » power of EBA is contained in article 9(5) of EBA's founding Regulation (Regulation 1093/2010), but this requires an enabling provision in relevant sectoral legislation in order to be activated in the sector concerned, in this case payment services, see for example article 41 of Regulation 600/2014 on Markets in Financial Instruments.

3.c) Creating an EU-level supervisory body for Open Banking, like the UK OBIE

In this option a new EU-level supervisory body would be created to oversee and enforce the implementation of Open Banking. This body would be either a new regulatory agency or an additional task for an existing such agency, such as EBA. It would be inspired by the experience of the OBIE created in the UK, and would have direct enforcement powers in the OB area, including powers to impose penalties for non-compliance. Due to constraints in the EU budget, it would be funded entirely from fees and sectoral levies.

5.2.4. Improve (direct or indirect) access to payment systems and bank accounts for non-bank PSPs

Other than the baseline, three options are considered. Option 4a) can be combined with 4b) or 4c), while 4b) and 4c) are alternatives (as 4c) includes 4b) but with extra features also).

4.a) Reinforcement of the right of PIs and EMIs to access to payment systems via an account with a credit institution

This option would involve strengthening the access of PIs and EMIs to accounts with credit institutions (i.e. banks), which allow inter alia, indirect access to payment systems to which the PIs and EMIs lack direct access. This would require amending article 36 of PSD2, which concerns PI and EMI access to accounts maintained with a credit institution. Currently, that article requires banks to provide the competent authority with duly motivated reasons for any rejection of access to PIs and EMIs, but does not require any explanation of withdrawal of existing account services and does not provide for a right of appeal. Article 36 could be modified to create a strongerentitlement to an account for EMIs and PIs[104] to cover also withdrawal of services, and also to place a stronger burden on banks, only allowing them to refuse or withdraw account access to PIs and EMIs if they have a material justification for such refusal or withdrawal (but with a possibility for a smaller bank to decline to manage an account for a PI or EMI where the high cost of servicing the account could have a significant impact on its overall profitability). Such justification could be for example breaches of law by the PI/EMI or reasonable grounds to suspect unlawful activity by or via that PI or EMI. Finally, it would be made possible for central banks, at their discretion, to safeguard funds held by Payment Institutions, providing a further fallback solution in case a non-bank PSP still finds it impossible to obtain an account with a bank.

4.b) Granting of direct participation of PIs and EMIs to all payment systems, including those designated by Member States pursuant to the SFD

This option would involve making changes to both SFD and PSD in order to remove the barriers to participation by PIs and EMIs in payment systems designated under SFD, namely

[104] Including during their licensing stage, where a bank account is already indispensable to safeguard future client funds.

adding PIs and EMIs to the list of entities which qualify as "institutions" in SFD, and deleting the provision in PSD2 (article 35.2(a)), which exempts SFD-designated systems from the obligation to have admission rules which are "proportionate, objective and non-discriminatory". It would not impose any specific requirements on payment systems, except the existing requirement in article 35 of PSD2 that the rules of payment systems must be "objective, non-discriminatory and proportionate, and that they do not inhibit access more than is necessary to safeguard against specific risks, and to protect the financial and operational stability of the payment system". It would clarify that PIs and EMIs are not admissible to participation in SFD-designated systems which are not payment systems[105]. However – as is the case today for payment systems which are not designated under SFD – no further guidance or requirements would be placed on payment systems, which would be free to develop their own procedures for ensuring that this general requirement is respected. All procedures and possible risk assessments prior to admission to participation would be left to individual payment systems.

> 4.c) As option 4.b) but with additional clarifications on procedures for admission of new members to payment systems, including the carrying out of risk assessment

This option would go further than option 4b): in addition to changing SFD and PSD2 to make direct access to designated payment systems possible for PIs and EMIs as under option 4b), it would involve laying down rules for the pre-admission process for applicants for participation in payment systems, including for example the risks for which an assessment must take place (operational risk, credit risk, liquidity risk, settlement risk and business risk), while avoiding discrimination and disproportionality between different categories of applicants (credit institutions, PIs and EMIs) and reinforcing the rights of rejected applicants for participation, including an appeals process. The POND principle would still apply to such assessments[106]. This would require the designation of a competent authority to hear such appeals and, if appropriate, impose penalties on payment systems for breaches. This option would build on and develop further the current requirement in article 35 of PSD2 that the rules on access of PSPs to payment systems must be objective, non-discriminatory and proportionate, and not inhibit access more than is necessary to safeguard against specific risks, and to protect the financial and operational stability of the payment system.

---

[105] It would do this by clarifying in SFD that PIs and EMIs qualify as "institutions" but only for systems which execute instructions for transfer of money or funds, not those which execute transfers of title to or interest in securities. SFD covers two kinds of systems, payment systems and securities settlement systems. PIs and EMIs have no need of participation in securities settlement systems.

[106] The POND principle in article 35.1 lays down that the rules of payment systems must be Proportionate, Objective and Non-Discriminatory.

6. WHAT ARE THE IMPACTS OF THE POLICY OPTIONS AND HOW DO THEY COMPARE?

6.1. Strengthen user rights and protection against fraud

6.1.a) *Measures to improve the application of SCA*

Regarding current exclusions from the scope of application of SCA, it would be very effective to include in the legislative initiative a clear definition of MITs and MOTOs and clarification on the treatment of these transactions, as a clear delineation of the scope of application of MITs and MOTOs, resulting in SCA covering a greater number of operations, directly increases the level of consumer protection against fraud. Absent the introduction of a clear regime in the directive, there is a risk that lack of clarity for stakeholders and competent authorities and abusive practices would persist in respect of MITs and MOTOs, with operations being unjustifiably not subjected to SCA. At the same time, payment sector stakeholders, which largely asked for more clarity on the regulatory treatment of these transactions, would have the legal certainty that they needed to apply SCA at the set-up of the mandate, without the need to apply SCA for subsequent merchant initiated payment transactions (MITs), and that only the initiation (not the execution) of payment transactions should be non-digital in order to not be covered by the SCA obligations (MOTOs). There would be no costs to PSPs, as the necessary investments for implementing SCA have been made, and covering certain additional operations by SCA has almost no incremental cost; this measure would therefore be efficient. The Commission has no evidence that the transactions which would be brought back to the SCA scope through these clarifications would cause more frictions into e-commerce (or costs due to lost business, in case of frictions occurred) as, two years after its entry into force, end-2020, SCA seems to be increasingly accepted and understood by the EU population as surveys indicate[107]. This option would be coherent with existing Commission guidance and Q&A replies of EBA. Option 1a) should therefore be retained.

6.1.b) Legal basis for PSPs to share information on fraud and obligation to educate customers about fraud

Under this option, the voluntary sharing of payment fraud data should become common practice. The key benefits for PSPs would be an increased ability to leverage their collective knowledge and experience to better combat payment fraud and make informed decisions about their capabilities, fraud detection techniques and mitigation strategies. Sharing information about payment fraud, such as suspicious IBANs and fraud trends, would increase awareness and responsiveness, making the financial sector more resilient. By including a legal basis in relation to GDPR this option would also increase legal certainty among PSPs. Respondents to the targeted consultation (mainly from the banking sector) and the Payment Systems Market Expert Group sub-group on consumer protection (see Annex 2) are in favor of including a legal basis that would allow PSPs to share specific information of attempted

[107] For example the Belgian consumer association Test-Achats found, in early 2022, that only 18% of the Belgium sample surveyed found SCA either difficult or very difficult. And 80% agreed with having strong authentication methods.

and realized fraud, which would improve the ability of PSPs to develop tools to further reduce fraud on the domestic and EU level. The costs for PSPs participation in payment fraud sharing schemes vary depending on the type of initiative and may include membership fees, travelling costs, staff deployed, IT costs for the installation and set-up of a payment fraud sharing platform, etc. On average, these costs which are recurring on a multiannual basis range between € 1 000 and 50 000, plus 1 to 3 FTEs[108]. Under this option, participation for PSPs would be encouraged but still remain voluntary, therefore no additional costs are foreseen as compared to the baseline.

Regarding consumer literacy and education about fraud and the risks of certain payment instruments/methods, various respondents to the targeted consultation, including public authorities, but also the EBA in its Advice[109], note that awareness campaigns should be undertaken, in combination with other measures that could have a positive effect and further mitigate these types of risks. While awareness programmes will not be a panacea to the risk of social engineering fraud, they will certainly enhance consumer awareness about fraud and the risks of certain payment instruments/methods, at limited cost. In order to achieve this purpose, the option would be to introduce specific requirements in the legislation on educational and awareness programmes for fraud risks (also addressed towards employees of PSPs), as proposed by EBA, leveraging on those set out in EBA Guidelines on ICT and security risk management.[110] Similar to the EBA Guidelines on ICT and security risk management, the option would be not to include detailed and prescriptive requirements, as there is the risk that requirements would become obsolete very quickly due to the ever-changing nature of fraud related risks. The limited costs for implementing such programmes, which for the first time will have to be based on specific and harmonised requirements developed by the EBA would be recouped, even with a tiny reduction in fraud, given that total fraud losses have been estimated around €323 million per year and a substantial part of these costs are borne by the industry through refunds, through handling consumer complaints etc.[111]

Option 1b) is therefore retained.

6.1.c) *Extension of the provision of IBAN/name verification by PSPs from instant payments to all credit transfers*

The costs and benefits of introducing an obligation for PSPs to ensure the availability for payers of an IBAN verification service was thoroughly and recently assessed under the

---

[108] These figures are taken from the DORA Impact Assessment (p. 44) and present the costs for threat intelligence sharing schemes. Due to the similarity to voluntary threat intelligence sharing schemes, these figures are also considered representative in the context of voluntary payment fraud sharing platforms.
[109] *Ibid.*
[110] The EBA Guidelines on ICT and security risk management (EBA/GL/2019/04), which could serve as a model for the educational and awareness programs for fraud risks.
[111] The value of losses due to fraud was estimated by the EBA to be 397,593,378 euros in the period between the second semester of 2019 and the second semester of 2020 for credit transfers, cash withdrawals and card payments from the perspective of issuers. See the EBA's Discussion Paper on the EBA's preliminary observations on selected payment fraud data under PSD2, as reported by the industry, page 29.

impact assessment accompanying the Commission's instant payments proposal.[112] The expectation underlying the introduction of an IBAN/name check for instant payments in that proposal is that it will reduce the rate of transactions sent to a wrong payee as a result of fraud or errors. Under that proposal, if adopted, IBAN verification will have to be offered by all PSPs providing euro instant payments, which will therefore incur the implementation costs for setting up such a service. Under this option, it is anticipated that the approach developed by EU PSPs for IPs would simply be extended to other transfers, without the development of an entirely new system. Therefore, only PSPs which do not offer euro IPs (for example, those operating exclusively in non-euro area Member States) will incur the full costs of developing such a new service; other PSPs will only incur the relatively minor costs of extending the IBAN verification service to non-instant or non-euro credit transfers.

As reported in the impact assessment on instant payments, based on the feedback from the Netherlands and UK markets, where such systems exist domestically, it seems that an IBAN-name verification service would be highly effective in preventing errors and reducing certain types of fraud. Regarding the rate of transactions sent to a wrong payee as a result of fraud or errors, according to the provider of the IBAN-name check solution in the Netherlands, there has been an 81% drop in fraud/scams taking the form of invoice fraud, and a 67% drop in misdirected payments due to payer errors since the setup of the IBAN-name check service in 2017.[113] In the UK[114] between Q3 2019 and Q4 2020, on a trend-adjusted basis, for the largest PSPs offering the service to their clients, there has been a 31% drop of number of payments sent to a wrong payee. Given that the extent of APP fraud in 2020 for all SEPA euro credit transfers in the EU is estimated at approximately € 323 million, there is significant scope for reduction of losses incurred by EU citizens and businesses resulting from such solutions. The application of this measure to cross-border transfers (beyond euro instant payments) and non-euro transfers should contribute to mitigating the higher fraud rate for cross-border payments than for domestic payments identified in section 2.1.1, especially as regards invoice fraud.

The number of PSPs required to introduce IBAN verification for the first time (i.e. those not yet covered by the proposal on IPs as they do not offer euro IPs) is estimated as 1200-1300 PSPs[115]. For those PSPs, the implementation cost of this element is at the most the same as calculated in the impact assessment accompanying the Commission's proposal on instant payments[116]. Estimates of implementation cost in that impact assessment were essentially based on experience in the Netherlands and varied considerably from PSP to PSP. With respect to the solution implemented in the Netherlands, the two main implementation efforts required from PSPs involved (i) integrating an API, allowing for account name verification, into the PSP's online/mobile banking environment, and (ii) adjusting customer databases to

---

[112] SWD(2022) 546 final of 26.10.2022.
[113] SurePay, Factsheet; see also brochure available here: SurePay - Brochure SurePay Confirmation of Payee .
[114] CP21/6 Confirmation of Payee call for views (psr.org.uk)
[115] 900-1000 PSPs in the non-euro zone that do not offer euro credit transfers (and therefore do not fall under the obligation to provide IPs in euro under the Commission's proposal on IPs) and some 300 PSPs which are PIs or EMIs that do offer euro credit transfers, but are proposed to be exempted from the obligation to provide IPs in the Commission's proposal on IPs.
[116] SWD(2022) 546 final.

ensure that the algorithm can match the payment data provided by the payer with the customer data of the payee's PSP. The one-off implementation cost ranged between € 10 000 and € 2 million (an outlier figure), which can be explained by the fact that some of the larger PSPs tend to have many more legacy systems that require adjustments, while smaller newer PSPs have newer, more agile technological capabilities and hence lower cost. Recurrent costs in the Netherlands ranged between several thousand euro per year to € 350 000 per year (again, an outlier figure from one major bank), with fees paid to the service provider per check performed constituting the largest part.

Implementation costs for this measure are anticipated to be lower than those for implementing a similar measure for euro instant payments, since the legislative proposal on IPs will already require EU PSPs to collectively put in place an IBAN verification system for euro IPs, which will also be able to operate without major modifications for non-instant credit transfers in euro. Thus, the cost of collectively agreeing on parameters and rules for a pan-EU system, and other development costs, will not need to be repeated. For non-euro payments, the system selected for euro IPs can be replicated if desired. Thus, the main costs for the affected PSPs would be the implementation of an API to connect to the system, and the modification of customer interfaces to integrate the IBAN/name check feature. These factors point to a total one-off implementation cost near the bottom of the potential range, of the order of €50 million in total (1300 affected PSPs and an average implementation cost per PSP of €40 000).

Costs would also be partially offset by operational savings arising from a reduced number of complaints to be processed by PSPs, which are costly to investigate and may even involve goodwill payments (e.g. made by some PSPs to avoid reputational damage). Costs might also potentially be partially recovered from customer fees, but it is considered unlikely that many PSPs would charge for this service, as this would deter usage and obviate the potential fraud reductions (there is no charging for the service in the Netherlands and the UK). Moreover, the experience with the existing solutions (offered to EU PSPs by SurePay or SWIFT, or imposed on PSPs in the UK) demonstrates that such solutions can be designed in full compliance with GDPR. This option would thus be coherent with the EU data protection requirements, as well as with the proposal on instant payments. Option 1c) is therefore retained.

6.1.d) *Full reversal of liability between PSUs and PSPs for fraudulent authorised transactions*

Option 1d) would be in line with the expectation of consumer representatives. Some form of a refund right for the consumer was called for by BEUC in its response to the public consultation. In cases where the payer can provide evidence of being a victim of an APP fraud, the solution would be effective in providing adequate consumer protection, but without evidence, it would be difficult. It is unclear to what extent this option would result in a significant reduction in APP fraud; it might, only serve to reattribute the social cost of fraud without incentivizing payers to avoid taking unnecessary risks (moral hazard). Any reduction of fraud would be dependent on efforts from PSPs. Furthermore, a full refund right for all fraudulent authorized transactions could, in contrast to the principle of irrevocability enshrined in PSD2 (article 80), bring considerable uncertainty to payment systems and the finality of credit transfers. In terms of efficiency, this option would not require any major upfront implementation costs from PSPs. On the other hand, since in such cases the funds are

unlikely to stay on the account of the payee long enough for the funds to be recovered, PSPs would incur ongoing losses, which could represent a substantial share of the estimated APP fraud for all SEPA credit transfers, estimated at € 323 million in 2020. Option 1d) should therefore be rejected as being disproportionate.

6.1.e) *Conditional reversal of liability between PSUs and PSPs for fraudulent authorised transactions*

This proposal builds on option 1c, on IBAN verification. The shift of liability for APP fraud to PSPs in cases of failure by PSPs to apply the necessary preventive actions to avoid fraud (i.e., no functioning IBAN/name verification service) would be a strong incentive for PSPs to ensure the good functioning of this particular fraud detection/prevention measure, which, in turn, is expected to have a mitigating effect on authorised payment fraud. This option would also provide incentives for payers to remain vigilant on fraud and to avoid taking unnecessary risks when making payments, as they would still bear APP fraud losses in all other cases where the bank was not negligent. Thus, this option would not require any major upfront implementation costs from PSPs and would reinforce the other chosen anti-fraud options. In cases of impersonation fraud, where the relationship of trust between customers and their bank and the bank's name are abused by a fraudster, and only when the victim is a consumer (and not a business customer) and has reported the impersonation fraud to the police and to the bank, it is appropriate to grant a refund right to victims of such fraud against their PSPs, except where there is gross negligence or where the consumer is involved in the fraud. The compensation for impersonation fraud granted by four major credit institutions (on a voluntary basis) in the Netherlands amounted to €51 million in 2022, which based on the Netherlands having 4% of the EU population could mean up to €1 billion at EU level. It is a good compromise between consumer organisations which expect full PSP liability for all cases of fraud, whether transactions are authorised or unauthorised, and banks that do not consider it normal to bear any liability for cases where the payer technically and legally authorised a payment transaction.[117] Option 1e) is therefore retained.

Comparison of options aimed to strengthen user rights and protection against fraud [118]
Selected options are a) b) c) and e). Option d) is rejected

Option	Effectiveness	Efficiency (cost)	Coherence	Overall score
1.(a) Measures to improve the application of SCA	+	≈	++	+
1.(b) Legal basis for PSPs to share information on fraud and obligation to educate customers about fraud	+	-	+	+

[117] See for example: European Banking Federation, EBF response to European Commission Consultation on the review of the revised payment services Directive (PSD2), July 2022

[118] In this table and other such tables later in this document, the number of + and – signs indicate the scale of the expected effect of a particular option as regards the different assessment criteria. Effectiveness analyses the extent a particular option would contribute to the achievement of the respective (specific) objectives, and is considered to cover the expected benefits (including possible cost reduction). Efficiency (costs) on the other hand focuses purely on the cost side of the option, and as such can never be positive (can be negligible). Coherence analyses the alignment of each option with other EU policy objectives, other policy initiatives and existing instruments. ≈ means marginal or neutral effect.

1.(c). Extension of the provision of IBAN verification by PSPs from Instant Payments to all credit transfers.	+++	--	++	++
1.(d). Full reversal of liability between PSUs and PSPs for fraudulent authorised transactions	--	≈	-	-
1.e) Conditional reversal of liability between PSUs and PSPs for fraudulent authorised transactions	+	≈	+	+

6.2. Improve the competitiveness of Open Banking services

6.2.a) Requirement for a dedicated data access interface

The effectiveness benefits of this option include data being by default shared in a more controlled and secure manner. In terms of security, banks maintain that APIs are a safer method to share data and would prefer TPPs to use APIs only. Through APIs ASPSPs can limit the data made available to TPPs to that which is legally required (only payments data, not for example savings), which they are not able to do if data is obtained by TPPs via the customer facing interface (fallback) due to the other technique applied for gathering the data – screen scraping[119]. This change would thus support data and consumer protection.

Regarding efficiency, this option would require capital investments from those ASPSPs that have yet to build such a dedicated interface. According to the VVA/CEPS study the development of the now-available PSD2 APIs cost on average about €2 mln per entity[120], but this cost may be lower now, because since PSD2 came into force many providers of "off the shelf" OB APIs entered the market, so ASPSPs unable to develop a dedicated OB interface in house can acquire this expertise externally at competitive prices[121], keeping in mind that the IT infrastructures of banks can be more intricate than that of other types of service providers. Most ASPSPs across the EU have in fact already built dedicated OB APIs[122] (and sometimes

[119]"*Screen scraping is a technology by which a customer provides its banking app login credentials to a TPP. The TPP then sends a software robot to the bank's app or website to log-in on behalf of the customer and retrieve data and/or initiative a payment. Banks have less control over the data retrieved, which may go beyond account data regulated under PSD2 and may include any customer data available. While with an API, banks have greater control to share only the necessary data for the TTP's service and customers do not need to share any credentials with TPPs."(* Screen scraping: a balancing act for banks | Capgemini) - TPPs are obliged to only process the data they have a right to process (Article 5 (1) (b) GDPR). Any superfluous data must be discarded.

[120] The Study estimates total costs at 2.2 bn EUR for a total of 1125 organisational entities (133 banking groups and networks, as well as 992 smaller and medium credit institutions). This number differs from the EBA credit institutions register (4000 institutions for the EU, incl. non-EEA branches), which is due to the EBA credit register providing separate rows per subsidiary (not identifying groups as the VVA has done in their methodology). VVA controlled for subsidiaries from the same banking groups to avoid double-counting, under the assumption that subsidiaries also use the APIs from the larger banking group they belong too.

[121] According to a dedicated industry methodology, initial development of an API may cost as little as EUR 25,000 (see Charboneau, T., Calculating the Total Cost of Running an API Product, in API as a Product, Tips for Running and API-centric SaaS Business, Nordic APIs, 2021-2022).

[122] ESBG Feedback on PSD2 API Usage, 19 January 2023: *All of the members that responded to the consultation have built dedicated PSD2 APIs (584 ASPSPs in 13 EEA countries - BE, DE, DK, EE, ES, FI, FR, LT, LU, LV, NL, NO, SE)*; EACB PSD2 API implementation, 20 January 2023: 1921 credit institutions from 8

other value-added revenue-generating APIs), which would mean that, on an aggregated EU basis, the additional cost of this change would be limited. The total net one-off cost of this option for ASPSPs is estimated at €32 million[123].

There should be no need for TPPs to make any new investment since TPPs are already supposed to use the dedicated OB interface, if available, and not use the fallback[124]. Most TPPs, especially those that were established post-PSD2 in any case prefer APIs over fallback interfaces. Some older TPPs (ETTPA members) have some reservations about removing fallback access, but also favour data access via APIs, provided that these are compliant and functioning.

In terms of transaction cost, TPPs maintain that gathering data via an API call is normally cheaper (and five times quicker) than it is via a fallback interface, and also that the recurring cost of maintaining a connection to the fallback (maintenance) is 6 to 12 times higher than maintaining a PSD2 API connection[125]. Maintaining a connection to the fallback means continuous manual intervention and updating as the customer interface can be adjusted in small ways, but frequently and unannounced (unlike changes to the dedicated interface which have to be announced in advance[126]). A large majority of TPPs, including those currently using fallback interfaces, would prefer Open Banking via APIs. TPPs would save resources on the maintenance of the connections to fallback interfaces due to the mandatory implementation and use of APIs. The VVA/CEPS study concluded the maintenance of API-based products costs TPPs about €53 mln a year[127]. If we assume that interface connectivity is about 20% of this amount (€10.6 mln) then the costs for maintaining the fallback connection could be between approximately €63.6 mln and €127.2 mln annually. These costs would be saved/reduced under this option.

Mandating the implementation of dedicated interfaces has support from most stakeholders, from different sides. The removal of the fallback interface has much support from different stakeholders, including banks, NCAs, the EBA, and many TPPs too (although there are some TPPs that would like to keep the fallback as a contingency mechanism). Furthermore, the mandatory use of the PSD2 APIs would lessen the extra traffic on ASPSPs' customer interfaces from TPPs also using the customer-facing interface (besides the ASPSP's own

---

Members States, all implemented a dedicated PSD2 interface; EBF feedback 23 January 2023: PSD2 APIs EBF consolidation of Members' feedback: approximately >90% of members have dedicated PSD2 APIs (EBF has 33 members representing 3500 banks); There is some overlap in banks that are members of more than one member organisation, e.g. there are banks that are both member of EBF and of EACB.

[123] Approximately 5% of ASPSPs (4000) do not have an API now, and the average cost of €2 million, giving €40ml total cost, reduced by the removed cost of needing to maintain a fallback interface.

[124] The fallback interface is the contingency mechanism that the ASPSP is currently expected to provide "*for the event that the interface does not perform in compliance with Article 32, that there is unplanned unavailability of the interface and that there is a systems breakdown"* – RTS art. 33(1).

[125] Input from ETTPA. See also Nordigen (AISP registered in Latvia), 6 October 2021, Vitor Urbano – link: 5 reasons why you should say NO to screen scraping (nordigen.com).

[126] RTS on SCA and CSC, art. 30(4): […] *any change to the technical specification of their interface is made available to authorised* [TPPs], *in advance as soon as possible and not less than 3 months before the change is implemented*.

[127] Annex 10 of VVA study.

customers, see Chapter 2.1.2), lowering the costs for maintaining that interface as well, as scraping bots (also used outside of Open Banking) make up about a quarter of internet traffic on such interfaces[128].

This option also takes into account proportionality as niche ASPSPs (defined with criteria to be developed by the EBA) could obtain a derogation either not to develop an API (and thus only have their modified customer on-line banking interface and the obligation to provide an Open Banking permissions dashboard) or not to have any OB interface at all since it would be irrelevant to them as they are not (very) attractive for Open Banking TPPs. It is coherent with the choice for a dedicated interface in the initiative on Open Finance. Option 2a) is therefore selected.

6.2.b) Permission dashboards

Permissions dashboards would respond to concerns of consumers about their data under Open Banking, allowing them to manage their data permissions in a convenient way. TPPs would not be allowed to discourage their clients from using TPP services by, for example, insisting on the easiness of permission withdrawal via the dashboard. The annual costs of operating an Open Banking permission dashboard, a change supported by all stakeholders, are relatively low – consent management providers offer quotations between €3 000 and €12 000 annually)[129]. There are 4000 credit institutions in the EU[130], which would bring the annual cost of operating/maintaining these dashboards to a range between €12 mln to €48 mln. The implementation of a permissions dashboard is supported by all stakeholders, including consumer associations. This option is coherent with the requirement for similar dashboards in the Open Finance initiative and is strongly coherent with GDPR. Option 2b) is therefore selected.

6.2.c) Impose a single, harmonised, API standard for TPP access to account data

Option 2c, which would naturally be combined with option 2a, could be highly effective by facilitating data exchange and reducing errors and failures of API calls. It would make it

---

[128] Han-Wei Liu: Two Decades of Laws and Practice Around Screen Scraping in the Common Law World and Its Open Banking Watershed Moment, 30(1) Washington International Law Journal, 2020: "*Given their everyday use for a wide range of commercial and non-commercial purposes, scraping bots are estimated to account for nearly a quarter of all internet traffic.*". Also, statistics on Open Banking API calls from the UK versus the number of visits to the respective banks websites shows that TPPs make many more API calls than that people visit the ASPSP's website (OBIE API data: API performance stats - Open Banking and website traffic: Free Website Traffic Checker & Analyzer | Website Rankings (semrush.com). There is no centralised data available on API calls for ASPSPs or TPPs in the EU.

[129] A possible indicator for the costs of the consent dashboard may be found in the consent mechanism required by the electronic Privacy Directive (Directive 2009/136/EC – the 'cookie law'), which was evaluated by an external contractor in 2017 [LINK]: *The figure of 900 Euro of compliance costs needs to be understood as an average value across all size classes of businesses, across all industries, and across all Member States*. Although the estimate reported in the Deloitte study is very rough, it is considered "*realistic*" by stakeholders. Commercial providers' publicly available consent dashboards offer quotations range from anywhere between €250 and €1000 a month (3000-12.000 EUR per year) [https://www.dataguard.de/blog/consent-manager].

[130] EBA Credit Institutions Register (January 2023), EU credit institutions (subsidiaries counted separately) and non-EEA branches.

easier for future new TPPs to connect (i.e. lower market barriers due to standardisation). It would also require fewer regulatory resources to assess PSD2 compliance in the future. It is the choice made in the UK in its implementation of Open Banking. This option is backed mostly by NCAs, EBA and some non-EU-based stakeholders, whereas most EU-based ASPSPs and TPPs oppose this option, considering it to have high costs (but which they do not calculate precisely). It therefore scores relatively highly on effectiveness and coherence.

Regarding efficiency however, it must be noted that banks and other ASPSPs have already made very significant investments to put in place their current APIs[131]. Some are following one of the different market standards, which still allow for variation, and others are not following any market standard. This has led to variations among APIs. Imposing one single standard would involve choosing one of the existing standards or mandating market participants to develop a new one. If an existing standard were to be chosen, ASPSPs which currently follow that standard would not incur any adaptation cost, while those ASPSPs which, in good faith and without breaching PSD2, have not followed the selected standard would incur an adaptation cost, so the choice of standard would be highly delicate. Requiring a new standard would render the work done on all existing standards wasted. More fundamentally, imposing a single standard would mean abandoning the principle of technology neutrality and could risk being inflexible, not future-proof and hinder innovation, since new better standards for interfaces may arise in future. A majority of both banks and TPPs oppose the imposing of a standardised API. It should also be noted that this option would remove the business case for aggregators - as aggregators only exist in order to assist TPPs to navigate differing APIs of varying quality – but this is not a conclusive argument.

Costs of adaptation for ASPSPs would vary depending on the degree of divergence of existing APIs from the new or selected standard and would thus vary. As indicated by both ASPSPs and EBA[132], it would probably require extensive resources and investments from most ASPSPs[133], as they may have to build an entirely new OB API or fundamentally alter their current ones. For ASPSPs this could lead to the costs they have already incurred to develop an API being lost, if their current API does not correspond to the new single EU standard and cannot be easily adapted. The VVA/CEPS study estimated that the building of OB APIs has cost the ASPSP industry about €2.2 bn[134]. According to one of the most popular market standards currently available, NextGen PSD2 from the Berlin Group, over 75% of banks have implemented this standard[135] as of February 2022. Even if one were to select this most popular market standard as the one single standard to be implemented across the EU, which would be the least invasive route to take, but still not create a level playing field, costs would be high. Assuming an increased implementation of the standard over 2022 to 85% of all banks, approximately 15% would still have to change standards, implying a 15% of €2.2 bn, €330mln lost costs. Assuming 25% efficiency gains because of the new standard and

[131] Most banks have put in place dedicated APIs – see option 2a.
[132] EBA Advice, Ch.6, question 17, para 369.
[133] Data on this is limited and where provided, quite divergent (from "*3 to 8 million (or higher)*" by Finnish banks to 21 mln by a large French bank, to "*far in excess of 100 million*" by a GSIB). The study (Annex 8 and 10) on the basis of very limited data, estimates 2.2 bn EUR (for all EU ASPSPs).
[134] See footnote 13.
[135] The Berlin Group: Progress Report on Open Finance, status update; February 2022.

improved API development expertise, the ASPSPs that would have to create a new API could incur another one-off cost of approximately €250 mln.

Even the 85% of ASPSPs that have already implemented the Berlin Group standard would still have to implement adjustments to remove the current variations, if that standard were chosen. Assuming a 90% coherence among Berlin Group users, 10% would have to be adjusted. Applying the same API-efficiency gain of 25%, this would amount to around another €140 mln of cost[136], bringing the total to €330 mln lost costs and €390 mln additional one-off costs.

Bank API maintenance (recurring) is estimated to be about €280 ml annually. API standardisation does not necessarily lead to lower maintenance costs than banks are currently facing, although the API maintenance costs increase with usage of the API, and therefore would already increase as the demand for Open Banking grows organically (without any legislative intervention) resulting in more API calls, the driver behind the maintenance costs.

The biggest efficiency gain of this option lies with the TPPs, which would face a far simpler situation than they currently are with the different API standards and intra-standard differences. The TPP maintenance costs of €53 mln a year could thus decrease. However, TPPs would be faced with some adaptation costs as well to reconnect to the new standardised APIs, offsetting this saving. Although some TPPs would prefer standardisation, others prefer the status quo, fearing a costly transition to standardised APIs.

Another benefit of this option would be easier monitoring of compliance by NCAs. The API standard could even lead to less need for intervention by supervisors as ASPSP and TPPs can no longer have differing interpretations of what the API should or should not do. Supervision-related recurring costs are estimated at approximately 30 mln € by the VVA/CEPS study[137] and these costs would fall under this option, although it is not possible to estimate by how much because supervision related costs extend beyond just PSD2 API compliance.

This option would not be coherent with the choice made in the impact assessment on Open Finance, which is not to impose one single standard, but rather to require the development of different market standards (such as those which already exist in Open Banking).

Option 2c) is therefore rejected, despite high potential effectiveness, due to excessively high implementation cost for banks (ASPSPs) and limited coherence.

6.2.d) Specify in more detail minimum requirements for OB data interfaces

Option 2d) would be less effective than Option 2c), as it would not impose the implementation of an API standard, but it would be far more efficient, due to its much more limited implementation cost for ASPSPs which have already established varying interfaces

[136] 10% of €2.2bn, net a 25% efficiency gain, to be made by 85% of ASPSPs as the other 15% is building a new API.

[137] According to the VVA/ CEPS study (Annex 10): 3 million (rough) estimate for *Ongoing supervision fees for new TPPs* and 28 mln EUR of recurring costs for *Higher need for supervision in national administrations due to PSD2*.

(see below). It would not however be totally cost-free. ASPSPs, the large majority of which already have a dedicated OB API interface, would have to revise these APIs and make adjustments where necessary, e.g. by making more data points available, such as account-holder's name[138]. TPPs would have to revise their connections to the interfaces as well and make necessary adjustments. Although most ASPSPs provide APIs already, there are still TPPs that choose to make use of the fallback interface, usually because, TPPs claim, the data made available in the OB API is not equal to the data they can obtain via the fallback interface (which would be breach of PSD2). This option would remove the time ASPSPs and TPPs currently spend on discussing what the OB API should provide, as the legislative text would clarify and specify which data is to be made available to TPPs. It would also facilitate easier monitoring and enforcement of the interfaces by NCAs. Furthermore, this option limits the changes that ASPSPs and TPPs have to make to some adjustments to the pre-existing APIs (instead of having to build entirely new APIs if a (new) API standard were imposed). ASPSPs would still be able to adjust their interface individually as long as it complies with the requirements set in the legislation.

In terms of costs this option may increase maintenance costs (due to greater usage of APIs because of the better quality), but market research already indicates that the market and demand for OB – and therefore API usage - is likely to grow, regardless of legislative intervention[139]. This option is therefore not expected to significantly impact the recurring maintenance costs.

One-off adjustments costs to ASPSPs (which would come on top of those recurring maintenance costs) can differ per ASPSP depending on its current API compliance and/or quality. A conservative estimate is that the cost of required changes can be between 1% to 5% of the costs of the building of the interface (see previous option) – between €20 000 to €100 000 per ASPSP. The lower end, 1%, is assumed for ASPSPs that need to make very few adjustments, who are already compliant with PSD2 and/or have simpler IT infrastructures. The higher, 5%, is assumed for ASPSP that might not be compliant with PSD2 and have to

---

[138] There are ASPSPs that do not make this information available through the Open Banking channel, despite the account holder's name being available in their own online channels. As account holder name does not constitute sensitive payment data for the activities of PISPs and AISPs, there is no reason for ASPSPs not to share this information, see also EBA Q&A 2018_4081 (responded to by the Commission). Some ASPSPs continue to argue that sharing the account name results in data protection issues, however by clarifying in the legal text that this key data point must be shared this problem and inconsistency would be resolved.

[139] According to market research (some explicitly presupposing legislative intervention stemming from the PSD2 review, some not) the OB market will continue to grow, legislative intervention or not. Market research from Juniper conducted in 2021 and publicly available at Statista here estimated a growth of Open Banking customers in Europe from approximately 18.2 mln users to 64 mln users by end 2024 (a 350% increase), regardless of regulatory intervention; Forrester estimated in November 2022, including assumptions regarding the increased adoption of Open Finance and increased standardisation stemming from the PSD2 review, that customer interest in Open Banking is "accelerating" as more and more Open banking solutions become available, such as consumer benefit checkers, funding of wealth management accounts, car dealership payments and more. Open Banking users in Germany, France, Sweden, Italy, the Netherlands and Spain combined are about 20 mln and project this will increase to over 70 mln users across these countries by end 2027 – link: Open Banking Adoption On The Cusp Of Robust Growth In Europe (forrester.com) // report: European Open Banking Forecast, 2022 To 2027 figure 1.

make more adjustments, that are larger and/or have more complex IT infrastructures. Of the ASPSPs that have a PSD2 interface, most have also received a fallback exemption[140] which is an indicator of a well-compliant API and therefore low adjustment cost. Therefore, most of the APIs already provided by ASPSPs will only have to make incremental changes to become compliant. The total one-off adjustments cost for ASPSPs is estimated to be €190 mln[141].

The recurrent annual maintenance costs for TPPs to maintain the connections to the PSD2 interfaces will probably decrease slightly, from the current amount of about €53 million annually for the entire EU TPP sector[142]. The one-off costs for TPPs to connect to new interfaces of ASPSPs which currently do not have them is estimated at a total of €24 million[143].

To summarise, the estimated one-off costs required to implement option 2c are estimated to be around €280 million for ASPSPs and TPPs combined.

This option would create an identical data set for all ASPSPs to provide access to, and thus more coherence. By combining the minimum requirements with the current "parity principle", this option would likely not result in a loss of Open Banking data options available to TPPs. Although ASPSPs might choose to lower the amount of available data by decreasing what is available in their customer-facing interface, "lowering" parity, in a way. As that would however also impact their own customers directly, this is not likely to happen.

This option, like option 2a), is likely to enhance the already anticipated growth of Open Banking. Regarding coherence, it should be noted that the Open Finance proposal does not choose to have any "parity principle" with customer interfaces, but this can be linked to the fact that in financial services outside banking and payment accounts, online customer interfaces are less common and much less frequently used.

---

[140] ESBG, EABC and EBF feedback received on members' PSD2 Interfaces.

[141] Assuming that the smaller and medium sized entities are likely to have outsourced their API development to external parties specialising in (PSD2) API development, it is assumed these (approximately 1000) are on the lower end of costs for adjustments (€20 000), giving €20 mln. The larger institutions (banking groups) also mostly follow standards and most have received fallback exemptions, which are only granted if APIs are compliant. However, given the size of these banking groups and some potential differences across their different APIs (due to different customer interfaces) their costs are estimated to be somewhat higher (€50.000 for 2000 entities), but as the APIs built in banking groups might be shared across subsidiaries there are some efficiency gains, assumed to be 20%, resulting in €80 mln adjustments costs for these groups. Lastly, there will be institutions that might have to make more significant adjustments due to more complex IT infrastructures underlying their customer interfaces and APIs. It is assumed 1000 entities would incur a one-off adjustment cost of €100 000 but enjoy some banking-group efficiency gains of 10% - somewhat lower due to complex IT infrastructures, resulting in €90 mln.

[142] VVA/CEPS study, 1.75 FTE. Based on feedback from TPPs the actual maintenance of access to accounts for APIs should take about 1 FTE day per year, which would mean about 30 mln EUR per year, and €6.500 per ASPSP.

[143] Conservatively, using the same assumptions as for ASPSPs, this option should take about 0,5 a FTE day of TPP work for ASPSPs that already have PSD2 interfaces with fallback exemptions and 2,5 FTE for those that do not. For the other ASPSPs (3000) this means a one off costs for TPP of €10 million and for those larger and/or more IT complex and/or less compliant ASPSPs (879) €14.2 million.

Option 2d) with sub-option 1, is therefore selected.

6.2.e) Abandon the non-contractual/no charging default principle

The choice for non-contractual relations by default between ASPSPs and TPPs aimed to avoid forcing ASPSPs and TPPs to agree thousands of bilateral contracts before OB operations can take place, or alternatively to agree a multilateral scheme with rules such as pricing. Furthermore, the data was already available via the direct interface (pre-PSD2 screen-scraping) and new, legally required contractual obligations would have increased the barriers to entry for (new) TPPs and have had an adverse effect on competition. This specific regime can remain in force after the application of the proposed Data Act, since the Data Act provides for sector-specific data access regimes.

Since PSD2 came into force, one argument given for low-quality APIs is the fact that the ASPSPs were not compensated for their expenses to design data access infrastructures. However, in the specific context of the existing PSD2 open banking framework, API structures have already been put into place by all operators, and it would appear unjustified to compensate them for past investments, which according to the study are estimated to be €2.2 billion, and ASPSPs have reported very differing amounts, ranging from a few million euro to *"(far) in excess of 100M"*[144] made to comply with PSD2. This needs to be balanced against negative impacts of this option: applying this option would seriously disrupt the current OB market, with ASPSPs and TPPs having to negotiate thousands of bilateral contracts (or else agree a scheme), which would almost certainly negatively impact TPPs' ongoing service delivery to consumers. Furthermore, it would have increased market entry barriers by leading to charging for all data access. It would also mean that data access services provided by ASPSPs to TPPs hitherto for free would, suddenly, become subject to a charge, with a new extra cost to TPPs which would negatively impact their profitability and could oblige some of them to stop their business. There would be no guarantee from data holders (banks) that this new revenue would be used to upgrade APIs.

This would be a total reversal of the approach taken in PSD2 and applied since 2018, risking significant upheaval possibly with a detrimental impact on the OB sector. It could also harm competition as many smaller TPPs would probably be obstructed by this financial barrier. The free access to data also means TPPs can keep fees that they charge to customers low, allowing more consumers and small businesses to benefit from OB services. The analysis of this option did not yield any concrete, quantifiable benefits for Open Banking.

Regarding coherence, it should be noted that while a scheme will be required for the Open Finance (OF) initiative, the circumstances are very different as OF, being a new market, has no 'legacy' no-compensation regime, and no investments in APIs have yet been made. OF, starting as it does from a 'blank sheet' can choose to apply, from the beginning, an approach where data access is based on (multilateral) contracts and there is compensation for all data access, with a view to incentivising data holders to develop quality interfaces. OF data users will be accustomed to charging from the beginning. However, it should also be noted that under PSD2 today, and in future, voluntary contractual relations between ASPSPs and TPPs

[144] See also Annex 7: stakeholder consultation.

are not prohibited (even for prescribed data access), and they do sometimes exist. ASPSPs making available 'commercial APIs' (usually providing access to data that goes beyond parity with the direct interface, "value-added data") subject to a contract are still required to provide a non-contractual PSD2 interface.

Option 2(d) is therefore rejected.

Comparison of options aimed to improve the competitiveness of Open Banking services
Selected options are a) b) and d). Options c) and e) are rejected

Option	Effectiveness	Efficiency (cost)	Coherence	Overall score
2.a) Requirement for a dedicated data access interface	+	-	++	+
2.b) Permission dashboards	+	--	++	+
2.c) Impose a harmonised API standard for TPP access to account data	+++	---	+	≈
2.d) Specify in more detail minimum requirements for OB data interfaces	++	-	+	+
2.e) Abandon the non-contractual/no charging default principle	--	≈	+	-

6.3. Improve enforcement and implementation in Member States

6.3.a. Replace the greater part of PSD2 with a directly applicable Regulation clarifying aspects of PSD2 which are unclear or ambiguous

Regarding effectiveness, Option 3a) would provide a better level playing field across the EU payments market. PSPs would have to apply the same, consistent and clear set of rules directly laid down at EU level irrespective of where they are operating in the EU. Improvements in terms of regulatory arbitrage and market fragmentation could be achieved. In terms of efficiency, it would be very beneficial for payments stakeholders to be able to rely on directly enforceable EU law to enforce their rights and corresponding duties and it would remove and/or limit late transpositions, divergent interpretations, gold-plating etc. Regarding efficiency, it is true that it would require Member States to repeal most existing national provisions regarding payments transposing PSD2, which would take up resources, but this downside is outweighed by the advantages. Supervised entities would benefit from improved and timely feedback provided by supervisors as the revised provisions would be clear, up to date and easy to apply. By incorporating further details in the legal text or by redrafting to reduce ambiguities and gaps, a more consistent application would be achieved (unlike the experience in rolling out the PSD2 requirements on Strong Customer Authentication). Circumvention or misapplication of the requirements would be reduced. This option would be coherent with what has been frequently done in the field of financial services legislation, where Directives when reviewed have often been replaced with Regulation or a combination of a Directive and a Regulation[145]. Most respondents to the targeted consultation who

[145] For example, bank capital requirements, anti-money laundering and securities legislation.

expressed a position also supported this option. In several meetings with Member States[146], a majority of Member States expressed broad openness to this possibility and objections were expressed only by a small number (these objections were related to a desire to be able to adapt the rules to local circumstances rather than to concerns about the cost of repealing national implementing legislation). Option 3a) is therefore retained.

6.3.b. Strengthen provisions on penalties in PSD

Option 3b) would be effective in so far as it would strengthen implementation of rules and give competent authorities the necessary powers to intervene to enforce PSD2. The list of breaches requiring penalties to be available to authorities would be a clear indication to Member States of the need to intervene actively to enforce the rules (which was not always done for example regarding the implementation of the PSD2 requirements on Strong Customer Authentication). The EBA power to temporarily prohibit certain products in case of risk to consumers can reinforce its work in helping Member States with implementation and enforcement. In terms of efficiency, the option would require greater resources to be committed by Member States to enforcement proceedings but this would be limited in proportion to the single market benefits. Consumers could be confident that the payments rules are adhered to by supervised PSPs and that measures including penalties are imposed in case of violation of those rules. Various stakeholders in the public consultations have pointed to weaknesses in the enforcement regimes of Member States and the need for reinforcement. This option would also be coherent with what has been done in various areas of financial services legislation[147] in recent years following the 2010 Communication on reinforcing sanctioning regimes in the financial services sector[148]. It would also be coherent with the EBA Advice, which recommends strengthening the current provisions on penalties notably by clarifying that infringements of prudential and conduct requirements must be penalised. Option 3b) is therefore retained.

6.3.c. Creating an EU-level supervisory body for Open Banking

Concerning effectiveness, the creation of a dedicated EU Open Banking body (option 3c) would have various upsides: by requiring the direct involvement of ASPSPs and TPPs (through funding and expertise) these parties would have "skin in the game" and are likely to cooperate better given their increased influence; this body would ensure that specialised supervisors can dedicate all their time to Open Banking, which is currently sometimes signalled as an issue within national supervisors, which are often already strained in terms of resources (and relevant expertise). The resource need on national supervisors would fall. As this body would also assure harmonisation across Member States there would be less fragmentation and more efficiency gains for ASPSPs and TPPs, especially those active across borders. Downsides are that the body would need time to integrate the legacy of all NCAs currently dealing with the topic, which might impede its effectiveness. Furthermore, ASPSPs

[146] Meetings of the CEGBPI committee of 30/11/2021, 7/4/2022 and 21/3/2023. See Annex 2.
[147] For example, the proposal for a Regulation on Markets in Crypto Assets Regulation (MiCA) or the 2021 revisions of the capital requirements rules for banks (see impact assessment SWD(2021) 320 final).
[148] COM(2010) 716 final, accompanied by an impact assessment SEC(2010) 1496 final.

and TPPs would have to deal with multiple supervisory bodies, with one solely for the purpose of Open Banking, and in the absence of any EU budget allocated to new resources for agencies, the body would have to be 100% funded by PSPs, so they would incur a cost for financial contributions.

As regards efficiency, estimating costs is difficult but the UK OBIE can be used as an indicator. Initially estimated to require approximately £20 mln per year, it had already surpassed £150 mln annual cost by 2021[149], only a small percentage of which was recovered in fees and charges. The costs of an EU body would probably be much higher, also given 27 Member States and cross-border issues. The supervisory body might be made more effective by having enforcement or supervisory powers of its own, but that would mean division of supervision for PSPs between a new EU body (for Open Banking) and NCAs (for other aspects of PSD).

Regarding coherence, it may be noted that an EU OB body would fit best of all with Open Banking option 2.b (harmonisation of APIs), which has been rejected above. Furthermore, no such dedicated EU enforcement entity is proposed in the Open Finance initiative.

In summary, option 3c) would involve significant cost for EU PSPs in fees and charges, in the hundreds of millions of euro per year, given the need for 100% sectoral funding, and would face significant operating challenges which mean that it is not certain to achieve benefits outweighing the costs. This option is therefore rejected.

Comparison of options aimed to improve enforcement and implementation in Member States
Selected options are a) and b). Option c) is rejected

Option	Effectiveness	Efficiency (cost)	Coherence	Overall score
3.a) Replace the greater part of PSD2 with a directly-applicable Regulation clarifying aspects of PSD2 which are unclear or ambiguous	++	-	++	++
3.b) Strengthen provisions on penalties in PSD	++	≈	++	++
3.c) Creating a EU-level supervisory body for Open Banking	+	-	≈	≈

6.4. Improve (direct or indirect) access to payment systems and bank accounts for non-bank PSPs

Option 4a) (reinforcement of the right of PIs and EMIs to access to payment systems via an account with a credit institution) would aim to remedy difficulties currently encountered by non-bank PSPs to obtain an account with a credit institution. It would come close to establishing a right to a payment account with a credit institution for PIs and EMIs, placing a burden on banks to explain rejection or withdrawal of service to a PI or EMI, with substantiated reasons. The establishment of an appeal procedure for rejected PIs and EMIs

[149] Alison White, Investigation of Open Banking Limited, Independent report provided to the UK Competition and Markets Authority (CMA), 1 October 2021.

would constitute another deterrent to refusal or withdrawal of account service by banks. This option would aim to ensure that non-bank PSPs would always be able to find a bank to provide account services and not experience frequent disruption of service. Certain non-bank PSPs may prefer to have only indirect access to payment systems via a bank, because of specific costs, or liquidity or collateral requirements of payment systems for direct participation; non-bank PSPs need a bank account for the purpose of safeguarding customer funds. Non-bank PSPs strongly support this option, and many Member States also; most banks oppose it, but the cost for banks should be limited. Therefore, this option can be useful to PIs and EMIs in ensuring a means of access and is therefore retained.

However, access to payment systems via a bank, even where ensured, is still considered by many PIs and EMIs as inferior to direct access. First of all, the non-bank PIs must pay fees to their competitors, increasing their costs, and their competitors have access to information about their business volumes which may be useful to them. Access via a bank can also increase the time taken to execute transfers, which can be key in the area of instant payments, which must be executed within ten seconds of the order being received. Therefore, option 4a) cannot be a complete solution to the problem of access by non-bank PSPs to payment systems.

Option 4b) (granting of direct participation of PIs and EMIs to all payment systems, including those designated by Member States pursuant to the SFD) would allow PIs and EMIs the possibility of direct access to all payment systems, including those designated by Member States pursuant to SFD (which tend to be the key ones, essential to provide most retail payment services), under the condition that they fulfil the access requirements of the system. It would allow PIs and EMIs to offer instant payments as well. However, certain problems would remain, including the problem of recourse in case of rejection of an application for participation. It would also leave entirely in the hands of payment systems the exact nature of pre-admission risk assessment against specific risks. These drawbacks could hinder the full resolution of the identified problem, and at the same time could potentially increase risks in payment systems by allowing the participation of PIs or EMIs with particularly high-risk profiles.

Option 4c) (as option 4.b) but with additional clarifications on procedures for admission of new members to payment systems) would aim to achieve the benefits of option 4b) and at the same time to remedy these shortcomings. It would require payment systems to conduct a full and fair risk assessment before admitting new participants, whether they be banks or non-banks, and only assess risks which are applicable in the specific case (for example, non-banks are much less exposed to credit risk). It would also establish a right of appeal to competent authorities for rejected applicants for participation in payment systems. This option is similar to the approach which has been applied in the UK, where PIs and EMIs have been admitted to direct participation in key payment systems, both public and private, following a thorough risk assessment process; the first such non-bank participant was admitted in April 2018, several others have followed since, and no adverse consequences have been observed so

far[150]. A large number of stakeholders of all categories, including many Member States and the Eurosystem, support this option (see Annex 2)[151].

Only a combination of options can fully resolve the identified problem and ensure that potential risks are sufficiently mitigated. The selected option is therefore 4c) in combination with 4a).

Comparison of options aimed to improve (direct or indirect) access to payment systems and bank accounts for non-bank PSPs
Selected options are a) and c). Option b) is rejected

Option	Effectiveness	Efficiency (cost)	Coherence	Overall score
4.a) Reinforcement of the right of PIs and EMIs to obtain a bank account with a credit institution	+	≈	++	+
4.b) Granting of direct participation of PIs and EMIs to all payment systems, including those designated by Member States pursuant to the SFD	+	-	≈	+
4.c) option 4.b) but with additional clarifications on procedures for admission of new members to payment systems, including the carrying out of risk assessment	++	-	++	++

7. PREFERRED OPTIONS

The package of preferred options (summarised in §7.4 below) represents largely specific targeted amendments to PSD2, rejecting most of the more far-reaching options, which either are not backed by sufficient evidence of a problem (see Annex 6 on scope) or would be too disruptive and costly to implement for uncertain benefit (for example, options 2b or 3c). In addition to the individual impacts of the selected options discussed above, they should positively interact with each other in a number of ways. For example, the enforcement-related measures will also have a horizontal effect boosting the effectiveness of all the other selected measures in other areas. A reduction in fraud should contribute to the efficiency of payments in the EU, free resources in PSPs for use in other areas, and increase consumer confidence. On the other hand, the baseline path of not amending PSD2 at all would leave a number of genuine problems unaddressed. The package of selected options is analysed below in terms of effectiveness in tackling the identified problems, efficiency (cost) and coherence with other EU legislation and initiatives.

The flanking measures discussed in Annexes, such as the technical clarifications described in Annex 7, the simplifications arising from the greater alignment of the supervisory regimes for

[150] See Bank of England press release and document « Access to UK Payment Schemes for Non-Bank Payment Service Providers », of December 2019.
[151] See also a joint letter by various fintech federations on this subject dated 3 February 2023.

PIs and EMIs described in Annex 8 and the improvements to consumer rights and protection described in Annex 10, should also be understood as horizontal measures, part of all relevant combinations of options. Technical clarifications (including on scope), and the integration of EMD2 into PSD2, covered in Annexes 6-9, are related to general objective 3 (Single Market). Measures to improve access to cash in Annex 9 are related to general objective 5 (protection of payment system users). Consumer rights measures, related to general objective 2 (efficiency, transparency and choice) and 5 (protection of payment system users), are covered in Annex 10."

7.1. Effectiveness

Regarding fraud, the effectiveness of IBAN verification in reducing fraud and errors in payments in the Netherlands and the UK, where such a system already exists, was highlighted in the impact assessment accompanying the proposal on Instant Payments[152]. IBAN verification has already been proposed to be introduced for euro instant payments, in the Commission's legislative proposal on IPs, so its effectiveness in the framework of this initiative would concern other credit transfers and non-euro currencies. The conditional reversal of liability in cases where the IBAN verification service is not functioning, will reinforce this measure and encourage PSPs to avoid downtime of their IBAN verification service. The other selected anti-fraud options, measures to improve application of the SCA requirements and to facilitate PSPs' sharing of fraud information, will have incremental but real impact against fraud. A clear delineation of the scope of application of MITs and MOTOs directly impacts the level of consumer protection against fraud and the rights and obligations of the customers and the relevant stakeholders, regarding transactions where SCA rules were not being respected. Exchange of information can be expected to produce the same benefits as in existing national schemes, but these have existed for too little time yet for the exact benefits to be quantifiable. The combined impact of all of these measures should be a measurable reduction in payment-related fraud, especially authorised or APP fraud. The impact assessment accompanying the Commission proposal on IPs found that the potential benefit of an EU-level IBAN verification system for euro IPs would be potentially up to €209 million per year, assuming 100% replacement of regular euro credit transfers by euro IPs. This would leave only non-euro credit transfers liable to experience benefits from the generalisation of IBAN verification, and the reduction in fraudulent or erroneous payments could be assumed to be in the range of €100-150 million per year, given the small total volume of non-euro payments in the EU than euro payments. The other measures in this anti-fraud package will further contribute to reducing fraud; if the amount of APP fraud would fall by 10%, that could represent a reduction of €32 million per year[153].

The proposed changes and clarifications on Open Banking will provide important clarity on the applicable framework and in particular on what quality and functionality must be offered in PSD2 interfaces. They will also enable TPPs to provide better and more OB services, and facilitate a better customer experience (fewer bugs, errors and other technical issues) which will make OB more attractive to use, and as a result, the OB market to grow. However this

[152] SWD(2022) 546 final of 26.10.2022. See for example annex 5. See also section 6.1.c) above.
[153] Based on the estimation of €323 million of APP fraud per year ; see §2.1.1 above.

result is indirect as the proposed changes and clarifications cannot immediately impact consumer demand; a clear and supportive legal framework can promote the success of OB but not guarantee it. For this reason, more radical options were rejected due to the high associated cost, without guarantee of success. Minimal disruption on the Open Banking market and facilitating extra growth than already projected by market research and the protection of sunk costs implementing PSD2, has been a priority. It is anticipated that the selected options will enhance the already predicted growth trend of Open Banking (by up to 10%), as APIs become of better quality and safer, TPPs will be able to provide more, better and reliable OB services and become more attractive to consumers. This would mean increased benefits to TPP revenues and to consumers making use of OB services.

Good functioning of the single market for payments will be facilitated by the clarification in the legislation of multiple points where space for differing national interpretations existed (see annex 7), by upgrading the greater part of PSD2 into a directly applicable Regulation, and by the reinforcement of available penalties which will improve the capacity of NCAs to effectively enforce the rules.

Regarding direct participation in payment systems for non-bank PSPs, the experience of the UK demonstrates that such direct access can effectively increase competitive forces in the payment sector and stimulate innovation, while not negatively impacting financial stability. A wide range of PIs and EMIs are active in the UK, not only offering payment account services to consumers, but also for example merchant acquiring and Open Banking services. Many of these PSPs are also active in the EU with a license from an EU Member State, but experience practical difficulties to offer competitive services in the EU due to their lack of direct participation in key payment systems in quasi all EU countries due to SFD restrictions. For those PIs and EMIs choosing indirect access via a bank, the more stringent requirements on banks will make such direct access more secure.

7.2. Efficiency

The package of measures identified has been calibrated to involve a minimum of disruption to the payment services market and to keep implementation costs to a minimum, while still achieving the specific objectives.

On fraud reduction, it can be mentioned first of all that the proposal on instant payments already requires EU PSPs offering euro instant payments to provide an IBAN/name verification service with such payments. For EU PSPs offering euro IPs, there will be minimal additional costs to extend such IBAN verification service to other types of credit transfer, non-instant payments in euro and to all credit transfers in non-euro EU currencies. Exchange of information on fraud incidents can be carried out between PSPs at relatively limited cost, and national level schemes already exist in certain Member States[154]. The proposed limited changes to the liability regime, linked in particular to IBAN/name

[154] For example, in the Netherlands, a programme (« Protocol Incident Warning System for Financial Institutions ») was approved by the national data protection supervisor (Autoriteit Persoonsgegevens) in 2021. The Protocol is available here.

verification, can be implemented via amendments to the general account terms and conditions between PSPs and PSUs, when these are due for renewal.

The amendments regarding Open Banking have been selected with a view to avoiding a need for significant new expenses for ASPSPs which have already developed APIs to allow data access by TPPs active in Open Banking. Another important factor which influenced the selection of options is the fact that the Open Banking market is predicted to grow[155] and significant changes could negatively disrupt this already projected growth. The additional revenue stemming from this baseline growth is estimated to be around €3.6 billion for 2024 and €6.7 billion by 2027 (cumulative revenue €12 bn by 2024 - see Annex 3). Existing APIs may have to be upgraded in certain cases, but will not need to be scrapped and entirely replaced with new interfaces. There will be the possibility of derogations for niche ASPSPs from having APIs or from having an OB interface at all. So, the one-off cost to the ASPSP sector of aligning existing APIs to the revised minimum performance requirements will be limited, and the ongoing recurrent operating and maintenance cost will not be significantly impacted. TPPs will incur lower recurrent costs as they will have to spend less resources on the manual-intensive fallback interfaces due to low-quality APIs. The removal of the obligation to have a fallback interface will involve savings for ASPSPs, offsetting the costs of upgrading APIs. More enforcement by NCAs could require more resources, but NCAs will no longer have to handle requests for fall-back exemptions, and TPPs' complaints due to malfunctioning or poor API data access will be reduced in the future. Furthermore, the compliance assessment for NCAs will be simpler and more straight forward as legislation becomes clearer. Moreover, it can be anticipated in the future that increasing numbers of added-value APIs, outside the scope of payment legislation, voluntarily providing additional data and services subject to a fee, will be developed, thus bringing some revenue to the ASPSP sector offsetting the overall cost of developing and maintaining APIs; although the basic PSD interface must continue to be provided free of charge by default.

The changes regarding penalties for breaches of PSD can be anticipated to lead Member States to devote more resources in national authorities to the investigation and sanctioning of breaches of rules by PSPs, and could generate recurrent costs for a few additional members of staff for those authorities. However, the clarifications on various elements of PSD can be expected to reduce staff time spent analysing such unclear elements, which can compensate for this. The same applies for the upgrade of the greater part of PSD2 into a directly

---

[155] Juniper Research available at Statista assumes the number of OB users will grow, not (explicitly) considering legislative intervention link: Open Banking Market Data & Forecasting Report; Forrester estimated in November 2022, including assumptions regarding the increased adoption of Open Finance and increased standardisation stemming from the PSD2 review, that customer interest in Open Banking is "accelerating" link: Open Banking Adoption On The Cusp Of Robust Growth In Europe (forrester.com) // report: European Open Banking Forecast, 2022 To 2027 figure 1.
Allied Market Research April 2022 estimates the European OB market (incl. UK) to grow from around €7.1 billion end 2020 to €45.7 billion end 2030. Controlling for the UK (4.5 mln of the 20 mln OB users in Europe were from the UK, end 2021, and the UK is more advanced than the EU) the EU growth would be around €5.5 billion end 2021 and €38 billion end 2030 – link: Europe Open Banking Market Size, Share | Forecast - 2030 (alliedmarketresearch.com)

applicable Regulation (although this will involve the cost to Member States of repealing much of current legislation transposing PSD2).

Regarding direct access to payment systems, there will be some one-off costs incurred by payment systems faced with a significant number of applications for membership, and given limited resources for risk assessment, this may require payment system operators to adopt a staged approach to implementation, with only a few new non-banks joining such payment systems each year (this has been the case in the UK). It is not expected that payment systems will need to increase their staffing levels for this task. The requirements on indirect access will be of limited cost for banks, unless they reject or cut off account services to many PIs and EMIs. PIs and EMIs will be able to offer payment services more efficiently and cheaply if they have direct participation in payment systems, thus enhancing price competition in the payments sector.

7.3. Coherence

The selected options are coherent with and reinforce each other. For example, strengthened enforcement will contribute to the progression of Open Banking under the new rules. Many PIs and EMIs are involved in offering both account services and Open Banking services to customers; better access to payment systems will facilitate this and provide synergies. Reinforced anti-fraud activity will contribute to smoother functioning of payment systems in general and increase the confidence of consumers in new innovative services.

Regarding the coherence of the selected options with existing Commission legislation and ongoing initiatives, a detailed account can be found at Annex 12, but key examples are given below:

- *GDPR:* a firm legal basis for PSPs to exchange information on fraud, in line with GDPR, is provided. Concepts of "explicit consent" for treatment of personal data, "silent party data" and "special categories of personal data" will be clarified, in a way which aims to assuage concerns expressed by many payments sector representatives about the effects on payments of Guidelines of the EDPB on PSD2[156]. See Annex 7 for more details.
- *Markets in Crypto Assets Regulation (MiCA).* MiCA categories e-money tokens (EMTs), as funds and therefore payment transactions made with EMTs fall within the scope of PSD2. However, given the very specific nature of EMTs as a type of crypto asset (use of Distributed Ledger Technology etc.), a certain number of clarifications are necessary in PSD2 in order to ensure certainty about the application of certain requirements (such as SCA) to payments using EMTs. Annex 7 provides more details about these clarifications.

[156] EDPB Guidelines 06/2020. The European PSP sector expressed concerns about these Guidelines as potentially hindering the objectives of PSD2 in a joint public letter. See also the Evaluation Report in Annex 5, section 4.1.3.2.

- *Settlement Finality Directive (SFD).* The targeted amendments to the SFD and PSD2 described in options 4b) and 4c) will maintain coherence, but with the positive effect of allowing potential direct access of non-bank PSPs to payment systems designated under SFD, instead of preventing such access, as at present.
- *Data Act*. The Commission proposal for a Data Act, once adopted and in force, will establish a horizontal framework for fair access to and use of data. However, the Data Act (article 40) allows different provisions in sectoral legislation, and the requirement for Open Banking mandatory access to payment account data to be provided without the need for a contract (i.e. for free) is an example of this.
- *Commission legislative proposal on instant payments (amending the SEPA Regulation)*. The SEPA Regulation lays down harmonised rules and technical parameters for credit transfers and direct debits in euro. On 26 October 2022, the Commission adopted a proposal for an amendment of the SEPA Regulation promoting instant payments (IPs) in euro. PSPs offering credit transfers and direct debits in the meaning of the SEPA regulation, including instant payments, remain fully in the scope of PSD. A noteworthy element of the present initiative is the generalisation to all credit transfers in all EU currencies of the requirement in the Commission proposal on IPs regarding name/IBAN verification; this does not affect the proposal on IPs, as this initiative will not require IBAN/name check for instant payments in euro, only other credit transfers. Furthermore, direct access of PIs and EMIs to all EU payment systems would allow the extension of the scope of the proposal on IPs to include them (in a future review); currently, PIs and EMIs are excluded from the scope of that proposal because their lack of direct access to key payment systems, due essentially to SFD, prevents them from offering IPs.
- Regarding coherence with the *Open Finance Initiative (OF)* , it should be pointed out that this initiative (see section 1.3) has its own impact assessment, and builds on the lessons learned on Open Banking as identified in the review of PSD2. This is because the policy measures required to improve an already existing system of data sharing under PSD2 are not the same as those needed to design a regulatory system for a new activity in other parts of the financial sector. This has led to different approaches being adopted in certain areas. For example, for data to which access is mandatory this initiative proposes to maintain the current "contract-free/compensation-free" approach (see §5.3) while the OF initiative provides for compensation for access to mandatory data sets[157]. Different approaches can be applied in different circumstances while remaining coherent. However, other policy options selected in Open Banking are closely aligned with the choices in the Open Finance initiative; see the discussion under each option in §6.2 above. See Annex 6 for the question of whether Account Information Services and Payment Initiation Services more appropriately belong in PSD2 or the OF framework.

[157] See the impact assessment on the Open Finance initiative [insert reference after adoption].

7.4. Summary of preferred options

Objectives / *Policy option*	EFFECTIVENESS	EFFICIENCY (cost)	COHERENCE	OVERALL SCORE
Strengthen user rights and protection against fraud				
Options 1a 1b 1c and 1e *Measures to improve application of SCA, legal basis for exchange of information on fraud, obligation to educate customers about fraud, extension of IBAN/name check to all credit transfers, conditional reversal of liability for APP fraud.*	+++	--	++	++
Enhance the competitiveness of Open Banking services				
Options 2a 2b and 2d *Requirement for a dedicated data access interface; permissions dashboards; specify in more detail minimum requirements for OB data interfaces*	++	-	++	+
Improve enforcement and implementation in Member States				
Options 3a and 3b *Replace the greater part of PSD2 with a directly-applicable Regulation clarifying aspects of PSD2 which are unclear or ambiguous; strengthen provisions on penalties*	++	-	++	++
Improve (direct or indirect) access to payment systems and bank accounts for non-bank PSPs				
Options 4a and 4c Strengthen PI/EMI rights to access via a bank account; granting the possibility of direct participation of PIs and EMIs to all payment systems, including those designated by Member States pursuant to the SFD, with additional clarifications on admission and risk assessment procedures	++	≈	++	++

7.5. Other relevant impacts

The selected options should also have a beneficial effect on the competitiveness of the EU payments sector. Within the EU a better level playing field between banks and non-bank PSPs should create more competitive pressure on banks to improve their payment services across the board, and assist innovation, thus contributing to the competitiveness of the EU payments sector. As a successful and efficient Open Banking sector is increasingly considered a sign of a modern and competitive financial sector, OB is becoming a feature of many jurisdictions (UK, Australia, Singapore, Japan etc.). The selected options will be at worst neutral as regards the competitiveness of EU payment service providers on any non-EU markets. Services like payment initiation compete with payment cards and contribute to lowering acceptance costs for merchants. Reduced fraud will lead to reduced costs for the EU payments sector and thus indirectly contribute to enhanced competitiveness. Overall, it is considered that a well-functioning competitive EU payment market will indirectly contribute to the overall competitiveness of EU businesses also in the international context.

Concerning the geographical impact of the selected measures, only one measure, namely the IBAN/name verification (option 1c) will have a very distinct impact in different Member States; both the costs of this measure and the benefits (in terms of reduction of fraud and of erroneously mistaken payments) will occur largely in non-eurozone Member States, as the great majority of PSPs in euro area Member States will already be required to implement the measure under the Commission proposal on instant payments (and in that case are free to voluntarily offer it for non-instant credit transfers).

Regarding impacts on stakeholders, see Annexes 3 and 13. Improved efficiency and competition in payment systems, together with reduced fraud, should benefit consumers and SMEs in their capacity as users of payments, while the improvements to Open Banking should benefit the many Open Banking fintechs which are SMEs.

7.6. Application of the 'one in, one out' approach

By means of this principle the Commission has committed to offset administrative costs of new initiatives by reductions in administrative costs of other initiatives. However, the present initiative does not involve administrative costs for businesses or citizens, as the initiative will not lead to any increased oversight or supervision of PSPs, or to specific new reporting obligations above those already existing in PSD2. There are also no regulatory fees and charges arising from the initiative. It is therefore considered that this initiative does not generate administrative costs which require offsetting under the "One In One Out" principle (although it is relevant for "one in one out" in that it creates implementation costs). It may be noted that the bringing together of the legislative regime for E-Money Institutions and that for Payment Institutions will lead to reductions in administrative costs (for example, alleviating the requirement to obtain a new license in certain circumstances).

7.7. Climate and sustainability

No negative implications for climate of this initiative have been identified. The initiative will contribute to target 8.2 of the UN Sustainability Development Goals: "To achieve higher levels of economic productivity through diversification, technological upgrading and innovation, including through a focus on high-value added and labour-intensive sectors".

7.8. Fundamental rights

The fundamental right concerned by this initiative is privacy. Privacy is enhanced by the clarifications described in Annex 7, to improve alignment between PSD3/PSR and GDPR.

7.9. REFIT (simplification and improved efficiency)

The present initiative is based on an evaluation, to be found at Annex 5. As part of the evaluation and review process, opportunities for administrative simplification were sought. The main such simplification contained in the present initiative is the integration of the Second E-Money Directive into PSD2 and the large-scale reduction in differences between the regulatory regimes for EMIs and PIs (with some residual remaining differences, such as own funds requirements) – this exercise will involve a repeal of the EMD2. More details about this approximation of the two regimes is contained in Annex 8. The removal of the "availability of funds" service, a facility which is not currently used, will also be a significant simplification (see Annex 6). The clarification of rules on SCA and other clarifications (see

Annex 7), together with the removal of divergences arising from national transposition of a Directive, will also contribute to simplification.

8. HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED?

The initiative will provide for a review, to be completed five years after the entry into force. Regarding the specific objectives, the following can be said about monitoring and evaluation:

- *Strengthen user rights and protection against fraud*. Regarding payment fraud, the operational objective is a significant fall in fraud, both concerning unauthorised and authorised payments. On this subject periodic reports are produced by EBA.
- *Enhance the competitiveness of Open Banking services.* The objective as regards Open Banking is an increase in the usage of AIS and PIS services above the baseline predicted growth, and an increase in PIS as a percentage of all digital payments. However, no official statistics on Open Banking are produced in the EU, and information (of which the quality cannot be independently verified) is only available from private sector consultants. PIS-initiated payments are executed as SEPA or non-euro credit transfers; it is not currently possible in official statistics to distinguish the initiation method of a credit transfer. AIS does not generate any payment transactions, and is only traceable as an "API call", but data on API calls for all PSPs is not collected systematically by supervisors. The Commission, together with EBA, will explore the possibilities for producing better quality data on EU Open Banking, but in the meantime, will be obliged to rely on the same private sector producers of data which have been used for the present evaluation and impact assessment.
- *Improve enforcement and implementation in Member States*. This should be detectable in a reduction in complaints received by the Commission and NCAs from citizens or PSPs, and an increased rate of active investigation of complaints.
- *Improve (direct or indirect) access to payment systems and bank accounts for non-bank PSPs.* The objective is that all PIs and EMIs active in the EU should have access to all payment systems in the EU, including those designated under the SFD, and have access to a bank account. The success of this objective will be measured by the numbers and the percentage of PIs and EMIs with (and without) access to the most important payment systems operating in the EU, including TARGET2 of the ECB. As regards indirect access, the number of notifications by banks to competent authorities of refusal or withdrawal of account access to PIs and EMIs, and appeals by PIs or EMIs against such decisions of banks, will be important. This information will be obtained from PI and EMI representative bodies and national competent authorities.

Monitoring summary table

Specific objective	*Indicator*	*Source of information*
Strengthen user protection against fraud and abuses	Reduction in % of fraudulent digital payments	EBA data and reports
Enhance the functioning of Open Banking	Number of OB API calls; PIS-initiated payments as a % of all digital payments	Private OB consultancies
Improve enforcement and implementation in Member States	More investigations by NCAs based on complaints	NCAs, EBA
Ensure a level playing field for all PSPs regarding access to payment systems	Number and % of PIs and EMIs with access to key payment systems; appeals against bank refusal of account services	PI and EMI representative bodies; EBA, ECB; NCAs for complaints of denied access to bank accounts

ANNEX 1: PROCEDURAL INFORMATION

1. LEAD DG, DECIDE PLANNING/CWP REFERENCES

This Impact Assessment Report was prepared by Directorate B "Horizontal Policies" of the Directorate General "Directorate-General for Financial Stability, Financial Services and Capital Markets Union" (DG FISMA). The Decide Planning references are:

- PLAN/2021/12798 – FISMA - Payment services – review report on PSD2.
- PLAN/2022/892 - FISMA - Payment services – revision of EU rules (Directive).
- PLAN/2022/1630 – FISMA - Payment services – revision of EU rules (Regulation).

The initiative on review and revision of PSD2 was included in the 2023 Commission Work Programme published on 18 October 2022, as part of a package on "data access in financial services", together with a legislative initiative on Open Finance.

2. ORGANISATION AND TIMING

One single Inter-Service Steering Group (ISSG) dealt with both this initiative and the Commission initiative on an Open Finance Framework, planned for adoption together with the present proposal, although the two impact assessments are distinct. Three meetings of the ISSG were dedicated primarily to the present initiative; those meetings, chaired by SG, were held on 11 November 2022, 13 January 2023 and 14 April 2023 (the first two meetings to discuss the draft impact assessment and the third meeting to discuss draft legislative text). The ISSG consisted of representatives from various Directorates-General of the Commission: CNECT, COMP, EMPL, ECFIN, ENV, HOME, INTPA, JUST, Legal Service, Secretariat General. The contributions of the members of the ISSG have been taken into account in this impact assessment.

3. CONSULTATION OF THE RSB

The Impact Assessment report was examined by the RSB on 1 March 2023. The RSB issued a positive opinion with reservations on 3 March 2023[158]. The principal reservations (which have been addressed in this final version of the report) were the following :

> *"(1) The report lacks clarity on consumer demand for Open Banking and on the extent to which consumer confidence in data sharing and cybersecurity may affect uptake.*
>
> *(2) The report does not provide sufficient impact analysis, in particular on competitiveness, SMEs, consumers and Member States as well as the impact of the proposed flanking measures.*
>
> *(3) The report does not provide sufficient clarity, including granular analysis, on the costs and benefits for the preferred set of measures."*

[158] That Opinion has been published and is available at [insert link]. In addition to the principal reservations cited here, there were numerous detailed changes required.

Changes and clarifications introduced in this report following the RSB opinion and comments include the following:

- The problem analysis has been more aligned with the findings of the Evaluation Report; for example, it has been clarified that in Open Banking, passing on user data to unregulated fourth parties via API aggregators is not a problem as such, as long as there is explicit consent of the data subject, although it is perceived as a problem by banks (section 2.1.2.);
- Regarding Open Banking, it has been clarified that no reliable data on the size of the market or demand exists, and while consumers report concerns about security of data, the constant growth in the number of providers indirectly indicates strong demand (section 2.1.2.);
- Greater explanation of the impact (and the interaction with the problem definition) of the "flanking measures" described in Annexes 7 8 9 and 10;
- The scoring of options in the tables in section 6 has been reviewed in order to make the scores more useful in policymaking terms;
- Reports were introduced in Annex 2 of two further consultation events held in March 2023, of the Payment Services and Markets Expert Group (stakeholders) and of the Commission Expert Group on Banking Payments and Insurance (Member States);
- Regarding the generalisation to all credit transfers of the "IBAN/name verification" service, greater explanation of the cost impacts and the geographical distribution of the effects of the option has been provided, and more information has been provided about the coherence of this option with the Commission's proposal on instant payments (section 6.1 and Annex 12);
- It has been explained why cross-border fraud is much higher than domestic fraud, and how the proposed solutions can contribute to reducing the difference (sections 2.1.1. and 6.1.);
- The distributional and competition-related impacts of the selected options have been discussed in greater detail in section 7; an SME test has been inserted (Annex 13).
- The specific objectives have been redrafted to be more precise and measurable, and more distinct from the general objectives (section 4.2).

4. EVIDENCE, SOURCES AND QUALITY

A number of inputs and sources of data were used in the preparation of this impact assessment, including the following:

- Evidence supplied in the various consultations described in Annex 2 and on an ad hoc basis by stakeholders.
- Evidence provided by the European Banking Authority in its Advice of 23 June 2022.
- A study carried out by a contractor, Valdani Vicari & Associati Consulting, delivered in September 2022, "A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2). Contract reference FISMA/2021/OP/0002.
- Data obtained from private sector operators, especially in the field of Open Banking. Regarding Open Banking, it should be noted that in the EU (unlike in the UK for example) there is no public sector entity which publishes or centralises data on Open Banking, and complete reliable statistics on the EU Open Banking sector are therefore impossible to obtain.

ANNEX 2: STAKEHOLDER CONSULTATION

1. Consultation plan

In order to ensure that the Commission's proposal adequately takes into account the views of all interested stakeholders, the consultation strategy supporting this initiative was built on the following components:

1. An open public consultation, open from 10 May 2022 to 02 August 2022 [159];
2. A targeted (but nevertheless public and open) consultation, with more detailed questions than the public consultation, open from 10 May 2022 to 5 July 2022[160];
3. A call for evidence, open from 10 May 2022 to 02 August 2022 [161];
4. A targeted consultation on the Settlement Finality Directive, open from 12 February 2021 - 7 May 2021;
5. Consultation of stakeholders in a Commission-led group, the Payment Systems Market Expert Group (PSMEG);
6. Ad hoc contacts with various stakeholders, either on their initiative or that of the Commission;
7. Consultation of Member States' experts in the Commission Expert Group on Banking Payments and Insurance.

The results of each component are presented below.

2. Open public consultation on PSD2 (and open finance)

Introduction

This annex provides a factual overview of all responses received. Therefore, any opinions expressed reflect the views of the respondents and do not reflect the position of the European Commission or its services.

Key messages

The key messages from the public consultation shows card payments are still the preferred methods of payment, both in-store and online. The choice in payment services has increased, and there is an overall positive stance towards new entities and Big Techs entering the field, although concerns about power and data privacy are expressed. Open Banking services (AISP and PISP) aren't used a lot, due to a lack of awareness of their existence and data privacy concerns. Feedback further shows a discontent with a lack of transparency for cross border charges and fees, especially those including a currency conversion. SCA is regarded positively, but with some suggestions for improvements.

---

[159] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13331-Payment-services-review-of-EU-rules/public-consultation_en .

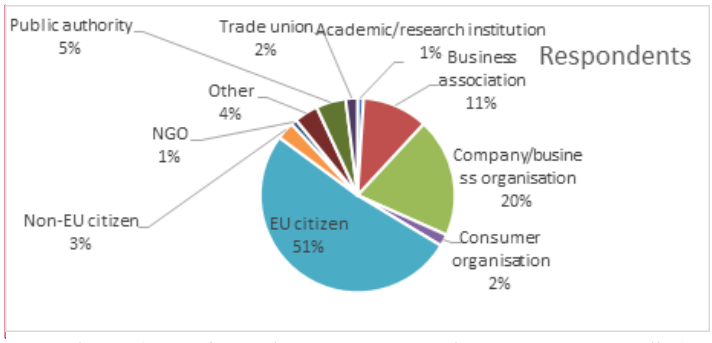
[160] https://finance.ec.europa.eu/regulation-and-supervision/consultations/finance-2022-psd2-review_en

[161] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13331-Payment-services-review-of-EU-rules_en .

The key message from the EBA Advice, after a quality control check on the responses is about how the PSD2 review should pay attention to transparency with regard to fees and charges related to cross border money transfers.

Summary of Public Consultation responses

Commented [KJ1]: This shape has been converted to an inline shape. Please check the position.



In total, 101 respondents (92% from the EU, 26 Member States, 93 replies) replied to the public consultation. EU citizens (52) formed the largest group of respondents, representing 50% of all respondents. Individual companies (20) and business associations representing their interests (11) formed the second largest group of respondents, representing together 30% of all respondents. There were also 5 public authorities, 2 consumer organisations (both EU-focused), 3 non-EU citizens, 2 trade unions (both EU-focused), 1 academic/research institution, 1 NGO (a charity) and 4 others who participated in the consultation (see Figure 1)

Many respondents indicate to be active in a non-defined field (Other – 43, Non-applicable – 20, total 62%), 28 respondents are active in Banking (28%) and 10 in Insurance (11%). Among those that labelled their activities as "Other" or "Non-applicable" are for example legal firms/lawyers, software vendors, EU-citizens involved in payments, associations for travel agencies, -vending machines and -telecommunications, and an association and an entity involved in electrical vehicle charging infrastructure.

Card payments are still the preferred methods for payment, both in-store (40%, cash being listed as the 2nd preferred method) and online (52%). Digital wallets on a mobile phone are only popular in-store (24%). Most respondents find the payment market innovative enough (51% yes – 48 replies, 30% no – 28 replies), and also find that the choice in payment services has increased over the last 5 years (70% yes – 66 replies). The overall sentiment towards new companies, including big techs, entering the market is positive, but there are concerns about power and data privacy, which is also reflected in the responses on the use of Open Banking (AISP or PISP) services.

A big point of critique regards unclarity about the costs and fees of making cross border payments (35% does not find these clear), especially those with a currency conversion (46% finds these unclear).

Overall there is support for the application of strong customer authentication (SCA), most finding it easy (in-store: 44%). It's deemed more cumbersome in an online-setting but considered acceptable given the fact that is prevents fraud. Respondents also find that SCA

has helped to make digital payments safer and more secure (50 replies, 76%). Some respondents suggest that more innovation should be allowed here, e.g. through the application of biometrics and behaviour, that PSPs should be required to offer non-mobile phone SCA solutions too, and that new security measures should be developed to counter new fraud methods such as social engineering and phishing.

For contactless payments without SCA most respondents indicate a wish for more control, in that users should be able to set their own (lower) limits, and that higher limits should be accompanied by a shift in liability.

Summary Call for Evidence responses

The Call for Evidence collected 195 responses in total, including one duplicate response. Further analysis showed that a large number of responses from Slovakia (72) and many responses not relating to the content of this CfE on the PSD2 review, but was in fact aimed against the Digital Euro (75, of which 62 from Slovakia). Another 3 responses were about tobacco. These responses were most likely meant for the separate consultations on the Digital Euro and on tobacco which ran at the same time as this one. A further 4 responses also did not appear to respond to the CfE on PSD2. Excluding these responses the final number of responses analysed is 113, of which 92 citizens (incl. 18 non-EU citizens, of which 8 from the UK), 12 business associations, 9 companies organisations and 1 consumer organisation.

The feedback from citizens mostly on cross border money transfers, and issues they are experiencing in terms of a lack of transparency. 74% (83/113) indicates they still face high fees when doing cross-border money transfers, with fees not always being clearly communicated upfront. Some citizens refer to money transfers with third (non-EU) countries, e.g. between the UK and the EU, but also within the EU between Euro and Non-Euro countries. Many responses were nearly identical, explicitly suggesting the including of a "mid-market rate" into article 45 of PSD2 (25 responses). Further analysis showed that one PSP providing cross-border money transfer services ran a campaign, encouraging its users to submit their feedback to the CfE on PSD2 regarding fees and transparency for these services. Their campaign included an explanation of the PSD2 review and a guide on how to respond, including some suggestions for responses.

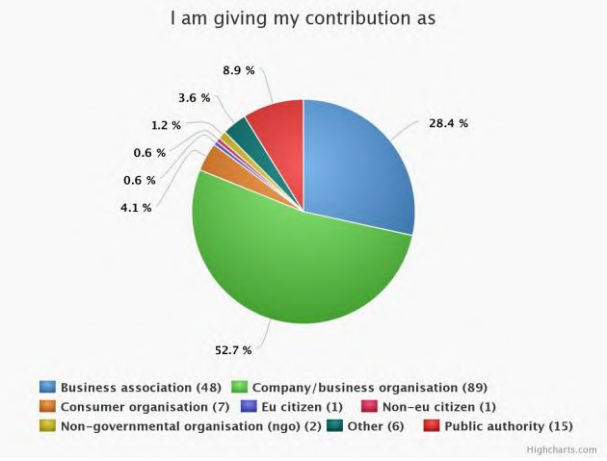
Other topics included in the feedback are about SCA, on its impact (fraud prevention), its implementation (incl. the limited use of SCA exemptions and the need for a mobile phone to perform SCA) and suggestions on how to improve it, mainly from the travel sector who request separate provisions for business travel. One respondent shares concerns about SCA and Electric Vehicle charging, related to the upcoming Alternative Fuel Infrastructure Regulation (AFIR), expressing a fear that the regulations could lead to disproportionally high investments for the providers of EV infrastructure.

3. PSD2 targeted consultation

Who responded?

The targeted consultation on PSD2 ran from 10 May to 2 August, 2022. A total of 169 parties responded to the consultation. There were 146 (86.4%) respondents from the EU (largest

contributors: 27 from Germany, 22 from Belgium, 15 from France, 12 from the Netherlands and 11 from Italy), 11 (6.5%) from the UK and 10 (6%) from the US.



4. Figure 4 Contributions given per type of stakeholder

To the right an overview of all contributions per stakeholders type, which included 7 consumer organisations (European and national ones) and 15 public authorities.

In terms of activity, most respondents labelled themselves as "Other" (98, 58%) and "Banking" (64, 38%). "Insurance" (5), "Accounting" (3) were also mentioned, among others. Among those labelling themselves as "Other" there were those active in Open Banking and APIs, E-money, Payment Service Providers, Retail, Telecommunications, Treasury and more.

Two responses appear to be duplicates, and due to the similarity of some responses it is clear some member associations have coordinated a "main message" or "main response". The duplicates have been controlled for during the analysis. Coordinated responses are considered unique contributions.

Key Messages

The targeted consultation (TC) comprised of 55 questions that covered stakeholders' experiences with the PSD2, whether the PSD2 objectives were met, targeted questions per PSD2 Title, and offered respondents the option to provide suggestions for changes to the PSD2. It should be noted that, despite a high number of total respondents (169), many respondents skipped questions or responded "Don't know"/No opinion/N.A. This is likely due various specific topics that were not directly applicable to all types of respondents.

It should also be noted that, with regard to the different questions and topics, views held within each stakeholder group are not always homogenous, meaning that drawing conclusions on group views is not always straightforward. Most noticeably, the group "ASPSPs" encompasses a heterogeneity of institutions, including credit institutions of different sizes and profiles, but also other types of non-bank PSPs which offer and service payments accounts, namely e-money institutions (EMIs) and payment institutions (PIs). One question where the views of ASPSPs have reflected this diversity (rendering meaningless an attempt to identify a group position) is, for example, on the level playing field. Here credit institutions' reported concerns largely focused on the obligation to provide a mechanism for TPPs' access to account data, whereas for non-bank PSPs a key issue concerned the

dependence on credit institutions to access payment settlement systems. Similarly, within the TPPs group, one often finds contrasting views between TPPs which practiced Open Banking already before the PSD2 framework entered into force and those emerging after PSD2[162]. One case of such differing views within this group concerned the data access mechanisms, where pre- PSD2 TPPs tended to make more use of fallback interfaces (thus favouring keeping this option), whereas TPPs emerging after PSD2 favoured quality, performing dedicated interfaces (either through common API standards, or by not opposing remuneration for data access services beyond a baseline in order to improve API quality).

The below summary of responses is provided in the same order as the Targeted Consultation itself.

General questions

In terms of the objectives of PSD2 respondents say the following: the majority of respondents, 85%(112/132) (excluding the don't knows/blanks) agree that PSD2 has been effective in making payments safer and more secure, in ensuring a high level of protection for PSUs across all EU (82%, 106/129), in increasing the choice between different types of payment providers (77%, 102/133), in strengthening consumer rights (78%, 98/126) and that it's been supportive in the creation of an environment that stimulates innovation in payment services (66%, 92/139). Especially regarding consumer and PSU protection, only a handful of respondents disagree (others are neutral/don't know).

Respondents are less positive about PSD2 improving the level playing field (30% does not agree, 56% agrees, out of 136 respondents). Some also comment that the PSD2 requirements, like SCA, are more likely to be implemented via smart phones, favouring this technology over others. The views are more nuanced for market integration and competition. There is a wider choice of PSPs than before (86% agrees 106/123), and the EU payment market is more competitive than before (77% 96/125). Respondents agree that the internal payment's market functioning has improved 62% (73/118). However, there is less support for PSD2 having contributed to the development of cross-border payments within the EU (43% agree, 50/115 and 37% are neutral 43/115). For remittances the number of responses was significantly lower (80 don't know, blank), and a large group remains neutral – 35% (31/89), against 38% (34) positive, and 27% (24) negative.

In terms of payment options and innovation the responses are positive: payment options have increased (78% (102/130) and making digital payments has become easier 66% (87/131), although views are less optimistic for international payments (EU and non-EU) – 35% (39) agree this has become easier. 71% of respondents agree that PSD2 has met its innovation-related objectives for the development of innovative payment services, solutions and overall innovation. An often-cited example is the rise of so-called (data) aggregators. Some remarks stressing a potential obstruction of innovation are placed with reference to the Level 2 text (RTS on SCA), such as the restrictive approach to behavioural biometrics (in the context of

[162] These sometimes diverging views are furthermore captured and expressed most notably by the two different associations of TPPs in the EU, ETTPA and OFA, with the former representing mostly TPPs which practiced Open Banking already before PSD2, and the latter those emerging since PSD2.

SCA), and that most authentication flows are still controlled by the banks. Furthermore, it should be noted that the uptake of Open Banking services is still low, although growing month-on-month.

A central aim of the PSD2 was to ensure and improve consumer protection, which respondents find the PSD2 has contributed to (82%, 102/125), including in that it has contributed to the protection of consumers' financial data (61%, 70/115). It has also led to a reduction in fraud in digital payments (74%, 86/116). However, all types of respondents identify the rise of new fraud methods that SCA cannot prevent (entirely), such as spoofing, phishing, etc. For surcharging (fewer responses), 62% of respondents (61/99) believe PSD2 has effectively removed these. Regarding clear information about payment services and terms and conditions only 50% of respondents (56/111) agree this now OK, whereas 29% remains neutral.

The costs and benefits are a more complex topic, with not much quantitative data, but many qualitative elaborations. Stakeholders agree that PSD2 has resulted in higher costs (89%, 72/81), often referring to the creation of PSD2 APIs and implementation of SCA. One level lower the PSD2 has mostly led to higher costs for merchants (66%, 52/79), and corporates (51%, 39/77). Less so for individual consumers (53% disagrees, 45/87). For the implementation of SCA the views are split: 36% (36/99) find the benefits related to SCA exceed the costs of its implementation, 38% disagrees (38/99). Concerning proportionality, the majority of respondents finds the investments to comply with PSD2 were disproportional to its benefits – 63% (64/101). Many banks (34) also find that the benefits of PSD2 do not outweigh the costs of implementation, often arguing the large costs placed on them to provide access to accounts for free. Lastly 71% of all stakeholders (65/91) disagree with the statement that PSD2 has simplified things (compared to PSD1).

In terms of enforcement most respondents, including NCAs and most banks and PSPs, consider that NCAs are sufficiently empowered to ensure the correct application of PSD2 (66%, 64/97), and to impose penalties (66%, 61/93). However, consumer organisations do not agree the provisions are adequate, and neither do some TPP respondents. A majority, including most banks and PSPs, (68%, 65/97) finds the EBA should conduct mandatory peer review analysis of the NCAs' supervisory activities, including the consumer organisations and TPP respondents. Most NCAs are against this.

Respondents could also provide suggestions for changes to the PSD2. 71% of them (95/133) believe PSD2 should be amended to cater for market developments, and that it should be complemented by self-regulatory measures and industry-led initiatives (72%, 91/126). Many also believe PSD2 could be simplified to reduce compliance costs (70%, 86/122). When asked if the PSD2 should rather be a Regulation, the majority of respondents remained neutral, didn't provide a response or doesn't know (43%, 73/169). Many respondents note that a full review of the PSD2 is still too premature, but that targeted amendments would suit better, such as behavioural biometrics being allowed as an SCA element or allowing banks to charge for the access to accounts (banks largely in favour, TPPs only for "value-added services"). Many stakeholders also note burden of the many different reporting obligations and request alignment between various pieces of legislation (e.g. DORA).

Title 1: subject matter, scope and definitions

This section covered questions about the scope (art. 1, 2) of the Directive, exclusions to the scope (art. 3) and definitions (art. 4). Most respondents (55%, 66/120) agree that the scope of PSD2 is adequate. However, 48/92 (52%) respondents believe the scope should change, which includes some that previously responded the scope was adequate. Some explanations refer to a merger of PSD2 and EMD2 and a closer look at the GDPR and access to accounts.

With regard to exclusions, many respondents believe these need to be modified (64/144 respondents, 56% disagree with the statement that article 3 exclusions are adequate). Those in favour of modifications (61/98, 62%) are largely active in banking (27/64, 42%). There is also more support for including *more exclusions* (68% agree, 47/69, 110 respondents do not have an opinion/no answer). Most of the respondents in favour of exclusions argue to be explicitly excluded themselves (e.g. a corporate bank suggesting an exclusion for a corporate card), but various stakeholders also report NCAs are applying exclusions differently (specifically the commercial agent, art. 3(b), limited network exclusion (art. 3(k)(i) and intra-group payments (art. 3(n)). Stakeholders that would rather see the exclusions narrowed down provide the argument that the PSD2 should reflect market developments and increasingly important positions some players are occupying (referring to certain technical service providers, such as wallets or TSPs processing large transaction volumes) and a level playing field. Some exclusions that received more attention over the last years were singled out in the TC: as regards the exclusion for telecom operators (art. 3(l)) the views are mixed: 23/89, or 26% find it adequate, 34/89, or 38% disagree. Concerning the same exclusion, the views are similarly mixed regarding the referenced limit to transaction values (€50).

On the question whether definitions are still adequate and do not need to be modified, the responses are mixed: 41% (46/111) agree and 42% (47/111) disagree. Specifically for art 4 – 66% (66/100) believe the definitions are adequate), but 5/7 consumer organisations believe something should be modified – but do not say what. Most public authorities are OK with the definitions (10/12 – 3 do not answer), but companies (52) have more difficulty (over 60% is OK with the definitions, 35% is not. Some suggestions to be reconsidered are "(remote) payment account" (should credit cards be included or not), "account information services" (clarify as the definition is only a subset of what is possible in AIS),

For Annex 1, the views on the adequacy of the list of services are mixed: 44% agrees (50/113), 38% disagrees (43/113). However, when asked about the specific 8 services the most frequent response is that no change is needed (approximately 83/122, 68%). Most noteworthy is the desire to change the description of account information services (17%, 21/122). A dedicated question was included on 'cash-in-shops', currently considered under cash withdrawals, and whether it deserved its own authorisation regime. Views were limited (many are unfamiliar with the service, it does not exist in all Member States), the majority has no opinion (55%, 63/115) and the others are evenly split (yes: 26/115, no: 26/115). Those in favour (mostly stakeholders active in banking and public authorities) argue it should be included in definitions, and that this service is important for access to cash in view of the continuous closing down of bank branches and ATMs. Those against argue that adding more regulation might discourage the provision of the service and that the service presents less risk and/or that the current regime is already proportionate.

In terms of expanding Annex I, some support is found for including the 'issuance of e-money' (41% agree, 52/126; 26 or 21% disagree), 'payment transactions using crypto assets

(including stable coins)' (50% agree, 63/126, 25, or 20% disagree) and 'digital wallet services (e.g. mobile apps for payments)' (43% agree, 54/126; 39, or 31% disagree). Some arguments provided in favour of adding issuance of e-money and digital wallet services are services are: creating a level playing field and simplification of regulation (concerning inclusion of e-money) and the fact that wallet providers have become increasingly interwoven with the provision of payment services, e.g. SCA depends on technical elements in mobile devices. No clear arguments are provided for the inclusion of payment transactions using crypto assets, although this may be related to the MiCA Regulation.

Stakeholder feedback also shows a reluctance to include certain services to the Annex, such as 'payment processing services' (24%, or 30/126 agree; 40% or 51 disagree), 'operating payment systems' (15% of 19/126 agree; 46%, or 58, disagree), and 'operating payment schemes (18%, or 23/126 agree; 40%, or 50/126 disagree) arguing that Oversight (ECB) already covers both of these services, and that the PSD2 is about services provided from a PSP to a PSU.

Title II: payment service providers

This section covered questions about authorisations and supervision. The level of responses was significantly lower for these questions, on average approximately 39% (66) of respondents provided a response, with 61% (103) of respondents leaving questions blank or "don't know". This could be related to not all respondents being regulated entities, but even regulated payment institution entities and third party providers and -associations provided "don't know/no opinion/not applicable" to e.g. the authorisation questions (e.g. *Q15: PSD2 is sufficiently clear in determining whether a service must be authorised or not*) or left the question blank. However, of those respondents that did provide a response, the majority find that the PSD2 is sufficiently clear in determining whether a service must be authorised or not (66% - 54/88), although there are 4 public authorities that disagree with this statement. 65% (51/78) finds the requirements to apply for an authorisation are adequate. Some respondents, including NCAs point out a need for clarifications, e.g. regarding the professional indemnity insurance, comparable guarantee, safeguarding requirements and ancillary credit, or suggest an introduction of e.g. a threshold regarding the amount of business to be provided in the home Member State (related to article 11) with the caveat that these thresholds should not be too rigid. Some authorities suggest changing the EBA Guidelines on authorisation to be converted into an RTS.

Regarding the dedicated authorisation and supervisory regimes for PIS and AIS the responses are mixed. Most find that the AIS regime is adequate (45%, 31/68), but 30% (23/68) disagrees, including some public authorities. There is no clear distinction in type of stakeholders, it's both public authorities, banks and TPPs that agree and disagree. Those that agree that the AIS regime is adequate mostly find the PIS regime adequate as well, and vice versa. A member's association of TPPs is of the opinion that the authorisation regime for these providers should be even more risk-based and suggests a lighter regime should be in place, arguing that these providers are not payment institutions, but providers of software tools.

The questions regarding capital and own funds received few responses, and proportionately many neutral responses too (between 35-45%). Most respondents find the capital and own funds requirements in article 7, 8 and 9 adequate. Some respondents point out that some Member States deviate in terms of capital requirements, such as France requiring TPPs (AISP

and PISP) to have the same 'capital projections' as Payment Institutions, although the provisions in article 9 do not apply to parties that only provide AIS or PIS, and some note that some Member States allow institutions to choose their own method of calculation, whereas others prescribe which one should be used. Various respondents request "payment volume" to be better defined.

A relatively large group of respondents found that PSD2 leads to regulatory arbitrage (47%, or 35 over 74), including some public authorities. Various respondents point out the authorisation process should become more harmonised across the EU, attributing the concentration in a few Member States to diverging national approaches. This point is also closely linked to another topic mentioned more frequently: agents, (triangular) passporting and home/host supervision (linked to article 19). Commercial stakeholders note that some host supervisors go beyond the passporting regime and impose requirements on entities passporting in their jurisdiction, although NCAs themselves do not indicate they deviate from any of the PSD2 requirements. In terms of triangular passporting, a large group of respondents (65%, 32/49) find it should be regulated with clear expectations and a division of responsibilities, shedding light on who is allowed to passport and who is not. A large consumer organisation is of the opinion that triangular passporting should not exist at all. Stakeholders in favour and not in favour of a triangular passporting regime are in favour of a register that allows NCAs to share data on an entity's passporting arrangements (maybe even including their use of agents), which would enable a host NCA to contact a home NCA and improve transparency.

Another grievance of payment institutions and EMIs is that they currently do not have direct access to SFD-designated payment systems, the result of a carve out (art. 35). A majority (38/55, 69%) would like to see this carve-out removed, mostly non-banks and public authorities. Those against are mostly stakeholders with direct access, often quoting financial stability risks and alleging PIs/EMIs are subject to "light" supervision and that non-banks already have access via intermediaries. There is no clear feedback on conditions or rules non-banks should be subjected to in exchange for direct access, except that it should be proportionate. There is also large support for the modification of article 36 (38/64, 59%), as many non-banks are not only having trouble getting bank accounts, but those with bank accounts are the victim of banks' efforts to de-risk (usually for the purpose of AML). 65% (47/72) are in favour of a mandate to the EBA to develop technical standards or guidance on art. 35/36.

Title III: Transparency of conditions and information requirements for payment services

This section covered questions about transparency; one of the objectives of PSD2 was to improve the transparency of conditions for providing payment services. Here too the level of responses dropped, although somewhat less than for Title II: approximately 58% of all respondents responded to the higher-level questions on transparency (the remaining 42% left questions blank – 48- or "don't know/n.a." – 23), where still fewer specific responses, i.e. yes or no, were received for the more specific- or in-depth questions. This could be attributed to not all respondents being subject to the transparency requirements.

A majority of respondents still found the requirements adequate and fitting current payment needs and methods (53%, 52/98; 32%, or 31/98 disagree) also finding the requirements contributing to making digital payments more secure (56%, or 52/93; 24% or 22/93 disagree). In terms of whether these requirements have led to a more informed user choice between

different payment products the views are split: 41% agree, but 37% disagrees (39 vs 35 out of 95). Views from consumer organisations in this regard are mixed (5/7 responded to these questions) but lean towards a more negative side (somewhat disagree and neutral).

In terms of changes to the requirements stakeholders from the banking sector call for a reduction of "information overload", which is a result also of other pieces of financial services legislation. In this regard a reconsideration or removal of the two-month notification period is mentioned. Respondents also call for clarifications, additional information and/or updates: for 'durable medium' a link to contractual terms should be sufficient, the inclusion of a benchmark mid-market exchange rate, informing the PSU in a framework contract under which circumstances funds can be blocked and released, clearer information relating to the name of the payee (related to commercial name) and more. Regarding the disclosure of currency conversion costs for one-leg transactions, most banks respond negatively to this requirement, arguing this adds complexity (as PSPs also have to comply with third-country regulations) and that this would go beyond the PSD2 geography, where most consumer organisations and public authorities are in favour.

Title IV: Rights and Obligations in relation to the provision and use of payment services

Title IV covers the rights and obligations of all parties involved within PSD2. This includes, inter alia, certain rules on applicable charges, irrevocability, the rights to refunds, rules for liability, and the requirements regarding access to payment accounts (who has access, how and under which circumstances). Furthermore, it contains requirements on operational and security risk and on strong customer authentication. Given the length and number of detailed articles in this Title the below analysis focuses on the larger topics of liability, access to accounts (Open Banking) and operational and security risks (incl. SCA).

A majority of respondents (between 57%-67%) finds the rights and obligations in PSD2 clearly written for both PSUs and PSP, but a relatively large group disagrees (20%-28%). Consumer organisations are not in agreement: some find the provisions are clear and adequate, some do not. Most public authorities find that these provisions are clear and adequate. A key topic mentioned by many stakeholders is "gross negligence", and that this must be clarified. The rules on applicable charges, one of the topics of the review clause (art. 108) are deemed adequate by most respondents (59%, 46/78). 7 respondents propose a complete prohibition of surcharging for all payments (not just cards) and a few others criticise the different application in Member States (art. 62(5)), both stakeholders suggesting the Member State options should be removed. Regarding the ceiling for contactless payments (56%, or 30/54, find art. 63 adequate) a majority finds this should stay the same (the cumulative limits of 150 euros and should remain: 46% or 44/96 and the total of 5 transactions 60%, 56/92), although a large group is in favour of higher limits. But consumer organisations argue two things: that consumers should have control and be able to (de)activate this function, or choose their own ceiling (max. 50 €), whereas another organisation argues limits are not needed given new payments means and COVID19-experiences and suggest that PSPs could

For refunds and liability, the views are more mixed. A large group of stakeholders finds the provisions on liability in PSD2 inadequate (35%, 33/95), mostly banks and banking associations, but also including 3 consumer organisations. For refunds 5 out of the 7 consumer organisations find these are inadequate (in total 42% disagree these provisions are

adequate; 39/92). A large group also finds that the allocation of responsibility is currently not adequate (51% agree, 47/93, but 27% disagree, 25/93), including 3 consumer organisations (2 others are neutral, 2 others agree). Another review topic was on the blocking of funds (art. 75) in case the final exact amount of the payment is not yet known at payment initiation: views are mixed and it is noteworthy that the largest group of respondents, which includes consumer organisations, banks, TPPs and public authorities indicates they don't know (45 respondents). A few respondents (6) explicitly request a maximum ceiling be introduced, whereas 21 other respondents emphasise that the introduction of such a ceiling would not work in practice. 3 respondents suggest to introduce a maximum time limit for the release of the payer's funds.

For access to accounts (Open Banking, OB), many stakeholders do not the regime successful (29% deem it successful; 32/110; 45% does not, 50/110), with no clear pattern or trend by stakeholder or country. On the other side most stakeholders do find that PSD2 ensures safe sharing of payments data (65%, 72/110), although some noteworthy respondents such as 4 consumer organisations (data protection concerns) and some banks disagree. The provisions on consent management and who is liable once consent is given leave room for improvement (51/108 or 47% and 47/103, or 46% are not content with the current provisions). Many respondents, including consumer organisations and banks request for banks to be allowed to provide a consent dashboard in their own interface to allow PSUs to have insight into consents given and the option to remove a consent. Stakeholders are also in favour of further clarifications on key concepts such as 'obstacle' (RTS on SCA & CSC, 77% - 64/83 in favour) and "objectively justified and duly evidenced reasons" (art. 68(5), 76% - 64/84). Those against clarifications are mostly active in banking (15/19 and 16/20, respectively). Many stakeholders suggest the confirmation of availability of funds (CAF, art. 65) should no longer be mandatory (or even removed), as this service has not taken off – this was also reported in CEGBPI. A similar request, for the removal of the mandatory requirement, is made for corporate payments (and corporate payment accounts), a request which overlaps with some reports of small or niche ASPSPs that have hardly seen any (or no) traffic on their PSD2 interfaces. When asked whether a common API standard should be included in EU legislation the views were split: 53% (49/92) is in favour – most public authorities and consumer organisations view this positively, 47% is against, consisting of a mix of banks and non-banks (incl. TPPs). In explanations many TPPs explain that APIs, even when following a market standard, still deviate somewhat and do not always work, nor provide the data fields necessary to provide the Open Banking-service. A few respondents also report a reliance of TPPs on technical service providers who provide the service of connecting to PSD2 APIs. Respondents also criticise the (lack of) enforcement in this area. Another important topic in this debate is remuneration (50% (47) in favour, 50 % against (47)), currently not allowed for Open Banking access. Banks are all largely in favour of changing this entirely, requiring a commercial incentive. TPPs appear to be OK with remuneration, but on the condition that only value-added services can be remunerated and that PSD2 "baseline" services remain available without contractual obligations. Many banks demand direct access (screen-scraping, or fallback) should be completely forbidden, whereas various TPPs require this should remain given the current quality of the PSD2 APIs, and require the removal of the fallback exemption too.

For operational and security risks, the majority of respondents finds the current provisions adequate (on average 75% agrees – on average 92 respondents provide an answer) and agrees with the statement that the framework has made payment service providers more resilient (74/97, or 76% agree). Noteworthy is that some public authorities are neutral (16%) and some don't know/left the questions blank (35%), with one public authority pointing out that many of PSD2's security requirements had already been implemented by the industry or through national legislation before the PSD2 went into force. Consumer organisations are less positive and remain either neutral or refrain from answering. With regard to fraud stakeholders indicate to be in favour of tools to enable better fraud detection, such as a data base or by enabling data sharing between PSPs.

PSPs also mention frequently that regulatory fraud reporting and operational/security reporting should be better aligned and harmonised internationally as they pose a large burden, also with an eye on DORA. Much feedback is provided on strong customer authentication (SCA): many stakeholders agree SCA has made digital payments safer (83%, 98/116), but do report it negatively impacted their business (51/93, 54%, or 56% report adverse impact), that it led to obstacles in the provision of services towards PSUs (52/77, 68%), including the exclusion of categories of customers/citizens (48/96 – 50%) and request SCA to be changed to a risk-based or outcome based model, to allow for behavioural biometrics and an inherence element and to provide clarity on which factors can be used to make up two-factor authentication. Concerns are reported about the newer types of fraud that SCA does not protect against, such as social engineering and phasing fraud and that Bigtechs and social media platforms should take responsibility too, as they allow malicious parties to use their platforms for fraud, e.g. by including links to those parties in their search engine results. It is deemed important to invest in consumer education and to consider how to deal with these new types of fraud.

Title V: Delegated Acts and Regulatory Technical Standards

Title V (art. 104, 105 and 106) covers the adoption of delegated acts and the obligation to inform consumer of their rights. These questions also returned a low response rate: between 56 and 66 respondents left these questions blank, and 43 to 66 respondents did not know/no opinion/n.a. (average response rate to yes/no: 52 respondents). Most examples and arguments provided in this section are anecdotal unless indicator otherwise.

Overall, 34% (38/113) of the respondents believe the requirements on delegated acts and regulatory technical standards to be adequate and 29% do not (33/113). Some suggestions for improvements were more precise and detailed RTSs, specifically referring to API requirements and SCA (and the related RTS and subsequent guidelines and opinion linked to this), for this type of delegated regulation to be more outcome-based and less prescriptive, to be reviewed more often, and to avoid fragmentation in implementation across Members States. Various stakeholders also comment on the work of the EBA in the field of harmonisation and the proceedings surrounding Q&As.

In terms of other field in which the EC could or should adopt delegated acts the responses were very limited (8/108 agree, 34/108 disagree and 60%, or 65/108 don't know). Arguments against include that relevant requirements should rather be set out in Level 1 text, that further delegated acts would only make things more complicated (mentioned multiple times), to

review relevant EBA opinions, guidelines and Q&As and consider to incorporate those in a future PSD3.

Concerning the informing of consumers of their rights (art. 106) the majority of respondents (excl. blanks and don't knows) is not in favour of changing these requirements, arguing that consumer rights are already covered by the PSD2, and that if any work on this should be done, it should be done at a higher level of EU legislation and ensure harmonisation across Member States to improve on the patchwork of local consumer protection requirements.

An additional remark was provided on consumer rights leaflets in paper (art. 106(3)) that was already shared with the Commission before the targeted consultation by various stakeholders. The paper leaflets are considered outdated and should be reviewed.

Title VI: Final provisions

The final provisions in Title VI include, amongst others, the provision on full harmonisation (see also question 8), the review clause, transitional provisions and amendments to other pieces of EU legislation. Between 103 and 129 respondents provided a response to these questions (incl. don't know/no opinion/n.a).

Regarding full harmonisation (art. 107) views are split – most stakeholders don't know or don't have an opinion (33%, 33/115 – mostly payment institutions, TPPs and 3 consumer organisations), an equally large group finds the provisions adequate (32%, 37 – a mix of largely banking-stakeholders, 18, payment institutions, TPPs and 8 supervisory and regulatory authorities), but a large group does not agree (19%, 22), of which most (11) are active in banking. In additional commentary some of the disagreeing stakeholders stated that PSD2 should become a regulation, others note the importance of ensuring harmonisation and the monitoring thereof across Members States.

Concerning the review clause of art. 108, 24 stakeholders indicated to have further items to be added to this clause (of which 16 unique responses). Items mentioned include the importance of level playing field (mostly by banks), (another review of) the rules on surcharging of article 62, access to payment systems, key payment infrastructure also having to capture providers of mobile devices, gateways and browsers given the changes in payment needs and methods, reviewing the interrelation of other regulations (like GDPR, DORA and AMLD). A consumer organisation finds the review should address the use and commercialisation of consumer data by intervening agents, but does not provide more detail. A large banking association stresses here, as also mentioned before under other titles by other (banking) stakeholders, the particular case of corporate payments and corporate payment service users, and how these differ from retail payments- and users, specifically for the (non-)application of SCA – arguing that corporate clients are more professional and both clients and payments subject to more security anyway.

With regard to the provisional provisions of art. 109 most stakeholders refrain from responding (56 don't knows -50%- and 58 blanks), similar to the question concerning amendments (art. 110, 111 and 112). The small group that responds deems the provisions adequate (29 respondents, 26%).

Finally, some other topics stakeholders deem important (besides repeating many points already shared in their response) and would want to highlight are the importance of cash to remain available, proportionality (banks vs. payment institutions and EMIs), a proper

consideration the implementation time schedules or regulation given past experiences with the PSD2 and the RTS on SCA and CSC, continuously increasing (overlapping) reporting requirements

4. Targeted consultation on the settlement finality directive

To support an ongoing review of the SFD, a targeted consultation was conducted between 12 February 2021 and 7 May 2021. It covered a number of aspects of SFD, including participants in systems governed by the law of a Member State[163]. Only this element of the consultation is covered here. The Commission received 72 responses to the targeted consultation (of which 62 covered the topic under discussion here). The majority of respondents were company/business organisation (41 respondents) and business associations (20 respondents). Together they represented 85%. In addition, nine public authorities and two academic/research institutions replied to the targeted consultation. No consumer organisation or citizen responded to the targeted consultation.

A majority of respondents agreed to add payment institutions and e-money institutions to the list of eligible (direct) participants in systems governed by the law of a Member State, at least as far as payment systems are concerned, although views varied as to under what conditions and requirements.

Of the respondents in favour of adding payment institutions and e-money institutions to the list of participants, the larger part (22 for payment institutions and 23 for e-money institutions) said that they should be allowed to be direct participants or indirect participants who may be considered direct participants if that is justified on the grounds of systemic risk. A smaller part (13 respondents for both payment institutions and e-money institutions) replied that they should only be allowed to be direct participants. One respondent said that they should only be allowed to be indirect participants. One respondent was against payment institutions being direct participants.

More than half of those that replied to the question (28 respondents) were against limiting participation to where it is warranted on grounds of systemic risk; 21 considered that such a limitation would be appropriate and 23 respondents were neutral, did not reply or did not express an opinion.

For both payment institutions and e-money institutions, a broad majority (35 respondents) rather or fully agreed that payment institutions and e-money institutions should be subject to a risk assessment; a smaller part (15 respondents) rather did not agree or disagreed with a specific risk assessment; four were neutral and 18 did not reply or did not express an opinion.

Moreover, a majority (29 respondents) rather did not agree or disagreed that payment institutions and e-money institutions should be subject to a particular risk assessment,

---

[163] The targeted consultation questionnaire is available at the dedicated Commission website: https://ec.europa.eu/info/consultations/finance-2021-settlement-finality-review_en. Other topics covered by the consultation were: third-country systems, technological innovation, protections of collateral security, settlement finality moments and notification of insolvency proceedings. The review of the SFD remains ongoing as regards those topics.

adapted to their particular risk profiles; 11 agreed with such a particular risk assessment; 13 were opinion and 19 or did nor reply or did not express an opinion.

5. Consultation of stakeholder groups

The Payment Systems Market Expert Group (PSMEG) discussed PSD2 on 16 December 2021, 5 April and 3 October 2022, and again on 30 March 2023[164]. A summary is provided by meeting, but topics that were discussed multiple times are not repeated.

In the meeting of 16 December 2021, members observed regulatory revisions should not be too prescriptive (focus on the "what", not the "how") and should be "time-neutral". They also found that PSD2 has increased competition, but has not yet reached all its objectives, e.g., the regulatory framework still appears to favour card-based payments over non-card-based payments and more standardisation is needed in terms of APIs, although members are not in favour of full standardisation. Members suggested that EMD2 and PSD2 should be merged and that AIS should be removed from PSD2 as this is data-related (GDPR). It was observed that PSD2 scope review should consider additional services such as Buy Now Pay Later, as well as wallet providers and custody services that are outside the scope of PSD2 currently. As regards technical service providers, some members found that they need not be in the scope, as they do not handle actual payments and only push data (and are covered by GDPR), while other members argued that their inclusion in the scope should depend on the type of their activity. Various members referred to difficulties with implementing and enforcing SCA and to the fact that enforcement varies across the EU and more harmonisation would be necessary (the same applies to AMLD and KYC). Members concurred that PSD2 needs to have sufficient protection measures in place to allow for safe and secure transactions, also in light of new market developments. Retailers observed that the contactless payment limits could be increased.

Several members observed that SCA has decreased the level of fraud, but whenever fraud occurs, the amount of money that is stolen is higher than before, especially in the access-to-accounts business (via social engineering, not card-based transactions). Many members agreed that PSUs need to be educated on fraud and fraud prevention and that collaboration within the industry would also be important. Members found that behavioural metrics should be considered as an inherence SCA-factor. Members also thought that SCA should not be too prescriptive as fraudsters use the requirements to base their workarounds on. If the framework were to allow for PSPs to determine the best combination of authentication methodologies, this could avoid a single point of failure.

The meeting of 5 April focused more on access to payment accounts (Open Banking), authorisation, transparency and rights and obligations. Next to issues already noted on 16 December, members note data-sharing issues within Open Banking related to the GDPR (e.g. data minimisation vs parity between online banking and PSD2). Furthermore, most issues members have encountered are grounded not in Level 1, PSD2, but in Level 2, the RTS on

[164] Minutes available at this link : https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&do=groupDetail.groupDetail&groupID=2287 .

SCA and CSC. Overall members experience few issues with regard to authorisation, although clarity on some topics, e.g. safeguarding requirements, would be welcome. Concerning transparency some members note how difficult it is to inform the payer upfront of the ultimate costs in case of a cross border payment with currency conversion, due to hidden fees in (inflated) exchange rates. Members support the implementation of IBAN checks to avoid potential mistakes made by the payer, and also warn that a right balance must be found between transparency and information overload for consumers. Also, members stress that framework contracts are not suitable for AIS and PIS. Under rights and obligations low value payment instruments (art. 63) were discussed and the blocking of amounts (art. 75), which leads to issues as funds sometimes take a long time to be released. Additionally, a consumer organisation argued that the limit of 50 euro (for not applying SCA during a contactless payment) should not be further increased and that consumers should be able to control this limit.

The meeting of 3 October 2022 was dedicated in its entirety to the PSD2 review. A number of subjects were covered:

- *Regarding the scope*, the discussion was about the exclusion of technical service providers, specifically pass-through wallets and payment processors, as they are becoming or have become important players (even when covered by outsourcing rules), and as consumers can confuse the user-facing-TSPs (like wallets) for being a PSP. For cyber resilience, specifically, DORA has a mechanism to allow critical TSPs to be brought into scope. Operators of payment infrastructures pointed to the ECB/Eurosystem oversight, both SIPS and PISA (still new), and stressed the need to avoid duplicate regulation. Entry into possession of funds was regarded as a clear criterion (for being in scope), and any other criterion should be equally clear, to avoid grey zones. It is important to clarify where liability lies and who must perform SCA. Trust is a key issue, but for the moment consumers seem to trust the providers with which they interface; there are few complaints.
- *Regarding open banking*, a majority of PSMEG participants, including many TPPs, opposed a single standardised API for Open Banking purposes, noting that PSD2 should be technology neutral and avoid regulating technical issues in great detail. Enforcement should be more proactive and effective. The absence of a dedicated enforcement body was pointed out. Regarding criteria on minimum performance and functionalities, bank PSPs tended to oppose excessive prescriptiveness in the legislation while TPPs tended to support more clarity about essential, or baseline, functionalities. Bank PSPs expressed discontent with the requirement to provide both an API and a fallback access, pointing out that APIs rarely crash; however other speakers challenged this and also added that APIs are not always complete, missing functionalities and/or data needed for AIS/PIS. Regarding possible compensation for access, particularly for value-added, or premium, features, many speakers referred to the SPAA discussions in EPC, and the challenges of both defining baseline and value-added features and determining compensation (while respecting competition rules but avoiding monopoly pricing). The risk of double charging for the same access (to TPPs and to customers) was mentioned. The importance of the Data Act was emphasised.
  Regarding fraud and consumer protection, the subgroup chair reported on the outcome of discussions on a number of consumer-related topics. No consensus had

been found on the user of the commercial or trade name of merchants in statements to users (complicated to implement), the IBAN verification system (costs to implement vs. its potential to reduce fraud), a common definition of "gross negligence" for social engineering fraud (although there was agreement on a public awareness campaign, relieving uses of liability could lead to moral hazard issues), blocked amount on payment instruments. Consensus was reached on financial inclusion and SCA (alternative methods of confirmation), increasing the upper limits for contactless payments but subject to user control and that imposing a maximum transaction time on one-leg out transactions would be extraterritorial and unrealistic.

The Commission asked about SCA circumvention, for example via the MIT or MOTO exemptions. The subgroup had not found examples of circumvention, but had looked mainly at non-EU operations. It was noted that the MOTO exemption was widely used, for example in the travel sector. *On direct access for non-banks to payment systems*, the lack of direct access of PIs and EMIs to SFD-designated payment systems, is considered problematic in terms of level playing field between banks and non-bank PSPs. The report made recommendations concerning direct access: to amend SFD article 2b and expand the catalogue of institutions following a risk-based approach and adjust article 35 PSD2 to align, and to explore the right for PI and EMI to safeguard client funds at central banks.
There were also three recommendations concerning indirect access:

- Amend article 36 as suggested by EBA: clarify offboarding and refusal to onboard. EBA should receive mandate to develop technical standards to determine criteria.
- Cover client funds at PI/EMA with DGS guarantee.
- Establish additional measures in safeguarding options that would create a more level playing field. Investing in low-risk assets, insurance, or a comparable guarantee.
- No opposition was expressed to direct access for PIs and EMIs, as long as risk-based access criteria are in place. A number of members considered that the existing risk assessment of credit institutions should form the basis for assessment of PIs and EMIs, mutatis mutandis. Non-bank PSPs tended to consider their credit and liquidity risk lower than that of banks (operational risk being the same) but were content to be assessed on the same terms.

In the meeting of 30 March 2023, in addition to a presentation by VVA/CEPS of its study, and updates from the different subgroups, the Commission presented the options under consideration, but without indication which options were preferred. Stakeholders expressed the following positions:

- On access to bank accounts for non-bank PSPs, those stakeholders who spoke were in favour of a combination of all the options. One stakeholder mentioned the need to introduce the possibility of safeguarding of funds with central banks. Another asked if there is any data available on bank refusals of accounts to PIs or EMIs. Another pointed out that PIs and EMIs tend to rely on the same bank, which involves risk in case of failure of that bank.

- On open banking, one TPP representative strongly supported the use by TPPs of the customer interface and condemned many APIs as being deliberately designed as unfriendly to TPPs. A different TPP representative expressed a different view, that well-functioning API access is essential and there is a need to move away from fallbacks and modified customer interfaces; there is a need for a resolution process in case an API is down, in their view. A banking sector representative opposed mandatory dashboards and supported a generalised move to use of APIs away from customer interfaces. Another PSMEG member pointed out that many smaller ASPSPs spend money on an API which is not used, and was against full API standardisation but in favour of more rules for APIs.
- On fraud, there was a presentation of a national initiative in one Member State to compensate consumers, with conditions, where they have been victims of Impersonation of Bank Employee fraud. Various different views were expressed on the appropriate balance of liability between PSPs and users in case of authorised fraudulent payments, and the usefulness of IBAN/name verification as a tool against fraud.
- The consumer subgroup considered that for contactless transactions, allowing consumers to set an individual threshold from 10 to up to EUR 50 would be complex and very expensive and not sustainable to implement (however, some PSMEG members expressed disagreement with this position). On Merchant Initiated Transactions (MIT), it was considered that these transactions should fulfil the following three criteria: (i) transaction with a fixed or variable amount and interval, (ii) governed by an agreement subject to SCA, (iii) that allows merchants to initiate subsequent transactions in the absence of the payer who is not available at the PoI (physical or online) to initiate and authenticate the transaction.

6. Bilateral contacts with stakeholders

A wide range of bilateral contacts were held with various stakeholders during the preparation of this initiative, essentially by videoconference, including BEUC - the European consumer organisation), payment services providers (banks, banking associations, European Payments Council, FinTechs, third party providers (TPPs)), Euro Retail Payments Board (ERPB), ECB, National Payments Committees, national central banks and supervisors, etc.

7. Consultation of Member States

National authorities were consulted in the framework of the Commission Expert Group on Banking Payments and Insurance (CEGBPI), which discussed IPs in a number of its meetings and provided input on the positions of Member States on specific elements. The CEGBPI discussed PSD2 in its meetings of on 30 November 2021 7 April 2022, and 16/21 March

2023[165]. CEGBPI members also provided over 260 pages of written commentary, mostly repeating points made during the meetings at a greater level of detail.

During the session of November 2021 CEGBPI members were asked how they viewed the developments in the payment market. Members reported an increased level of digitisation, which was considered to be reinforced by the COVID-19 pandemic. Many saw a rapid change in the speed of payments/transactions. Concerning the newer regulated Open Banking services members report new licences have been issued to AISPs and PISP, but the uptake of the services remains limited. All members agreed that a thorough review, and even revision of the scope of PSD2 was needed. Members reported that the differences between certain types of payment services have become more difficult to identify, reporting difficulties in assessing whether an entrant needs a licence or falls under an exclusion (in particular referring to TSPs and limited network providers). There was overall consensus that the EMD2 and PSD2 should be merged and the need for alignment of PSD2 with other pieces of legislation such as AMLD, MICA, DORA, Data Act, GDPR, DMFSD, etc. Some questioned whether PSD2 should cover also savings accounts, and others suggested to analyse the necessity of a group supervision similar to the CRD approach and considering a recovery and resolution framework for payment institutions and E-Money Institutions.

The introduction of the PSD2 has led to banks creating APIs and various members expressed the view that the Regulatory Technical Standards have not always facilitated an easy and sound convergent development of Open Banking across the EU. Some members agreed that having an EU API standard would have been useful. It was pointed out that between the implementation of PSD2 and now, banks have also started to use APIs for purposes other than laid out in the PSD2. Members remarked on the many challenges related to the implementation of the Strong Customer Authentication (SCA) and while it was considered still too early to fully assess its impacts, members have seen a decrease in the fraud rates. However, members remarked that new types of fraud (such as social engineering fraud) are popping up that are not captured by the SCA. Some members saw the need to consider additional SCA exemptions, e.g. if the payer uses an unattended terminal at charging stations for electric vehicles.

The session of 7 April was almost entirely dedicated to PSD, discussing scope, the supervisory framework, fraud prevention (SCA) and Open Banking. Members stressed the importance that a new PSD-framework would need to be future-proof and cover risks posed to consumers, and that various things could be clarified. Members sometimes struggle to qualify whether an entrant provided a regulated or non-regulated service, so precise definitions on the services of Annex I would be welcomed, as well as a clear definition on "payment account" and on "funds" and by including criteria, e.g. from the EBA Guideline, for the limited network exclusion. Regarding TSPs members are cautious – the PSD should focus on the provision of payment services, not ancillary technical services and referred to Oversight already covering operators of payment systems and schemes. Some members

[165] Minutes available at this link: https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?do=groupDetail.groupDetail&groupID=2885&Lang=EN .

suggested a taxonomy of technical services could be helpful, and to consider targeted requirements (e.g. strong customer authentication). The review should consider any risks coming from new payment solutions, such as digital wallet solutions or Buy-Now-Pay-Later, and if these should be included in PSD2 (members believe BNPL should be covered under the consumer credit directive).

As regards the adequacy of supervisory framework members agree that it is overall adequate, also agreeing that the rules for small payment institutions should be maintained, but some improvements/changes could be considered, for example on passporting (this should be timely) and on the professional indemnity insurance required for PISPs and AISPs. Feedback was also received in written form, where members stressed that the licensing process should not be subjected to a one-month deadline due to complexity and the quality of applications. From a supervisory point of view the removal of AIS to another framework (instead of PSD2) could lead to difficulties in supervision as different authorities may be in charge.

Regarding fraud, members require clarifications to the provisions on SCA, also discussing the new fraud methods (social engineering) that SCA does not protect against. Moreover, members request clarification on mail order/telephone order (MOTO) transactions and the need for legislation to clarify that the use of a mobile phone should not be a prerequisite for SCA and to prevent financial exclusion. Furthermore, it was discussed if the exemptions to SCA should not be moved to Level 1 (currently in RTS) and if more exemptions should be considered, for example for electronic vehicle charging stations.

For Open Banking many members suggest that having one API standard would be beneficial and, in the long run, facilitate competition, although members acknowledge the implementation might be costly and either designing a new unform standard or selecting one of the existing standards would be challenging. Issues with the amount and type of data to be made available, while remaining compliant with GDPR, were discussed (data minimisation, silent party data, processing of special categories of personal data).

It was furthermore considered by CGBPI members that a renewed payment framework might be in the form of a regulation as this might be beneficial for the market, needs a short implementation period and would be in line with other frameworks (e.g. MiCA).

In the CEGBPI sessions of 16 and 21 March 2023 (two half-day sessions), broad support was expressed by Member States for the extension of IBAN/name verification to all credit transfers in the EU, and to strengthened transaction monitoring and exchange of information on fraud among PSPs. Certain Member States felt that attribution of liability for fraudulent authorised transactions is a delicate matter, and moral hazard must be avoided. On Open Banking, only seven Member States took the floor, with a wide range of views expressed. Four Member States wished to maintain consumer protection rules in national law, not an EU Regulation, on the grounds that the possibility of adapting the rules to national circumstances is desirable. There was broad openness to the incorporation of rules for e-money institutions and payment institutions together in one legal instrument.

ANNEX 3: WHO IS AFFECTED AND HOW?

1. PRACTICAL IMPLICATIONS OF THE INITIATIVE

1.1 Introduction

The costs of the initiative have been kept to a minimum, via the rejection of the most costly options. Costs are mainly one-off implementation (adjustment) costs, and fall largely on ASPSPs (essentially banks). The most costly elements of this initiative, but potentially the ones with the greatest potential for social benefit, are those related to reduction of authorised (APP) fraud and to Open Banking. In Open banking, costs are offset by savings (such as the removal of the fall-back interface and of its exemption procedure) and by the adoption of proportionality measures (possible derogations for niche ASPSPs). The cost of improved enforcement and implementation will be limited and fall on Member States. The costs of direct access to key payment systems for Payment Institutions and E-Money Institutions will again be limited, and fall on the payment systems in question.

The benefits, on the other hand, are ongoing benefits and accrue to a wide range of stakeholders, including users of payment services (consumers, businesses, merchants and public administrations) and also PSPs themselves (especially non-bank fintech PSPs). They are harder to quantify, as they involve greater innovation and competition, with potential for lower prices and a greater variety of services on offer, plus reductions in APP fraud. As with PSD2 itself, the benefits are recurrent, while the costs are mainly one-off adjustment costs, therefore the cumulative benefits should exceed the total costs over time.

1.2 Payment Service Providers (PSPs) and other businesses

PSPs which do not offer euro IPs will be impacted by the cost of offering an IBAN verification service, averaging a few hundreds of thousands of euro per PSP in one-off costs (the cost is higher the bigger and more complex is the PSP), with annual maintenance costs averaging a few tens of thousands of euro per PSP. These costs can be offset by charging users for the use of this facility, and by reduced numbers of fraud-related complaints to deal with.

The increases in user rights and information (see Annex 10) will involve a small one-off adjustment cost (adaptation of standard contracts etc.) and limited ongoing costs, for example for provision of information in cases of ATM withdrawals on other networks and one-leg out operations.

Certain PSPs will incur a one-off cost for improving their API interfaces for Open Banking TPPs or creating one where one is not in place yet. The total cost of this for the ASPSP sector is estimated at €160 million. This will be offset by the saving of no longer having to make available a fallback interface or suffering additional traffic on the direct customer interface (see Chapter 2.1.2). Ongoing maintenance cost for APIs will not be directly impacted by the proposed changes.

PSPs which are Open Banking TPPs will experience the benefits of having defined quality and functionalities for APIs, thus enabling them to offer a better service to their users and supporting consumer adoption of OB. The TPP sector will experience a small cost around €24 million for adapting to new rules on interfaces.

PSPs will benefit from greater legal certainty due to a more detailed and coherent set of rules on payments which will be applied in a more effective way across the EU e.g. regarding criteria for penalties. They will be exposed to lower compliance costs over time as the rules on payments will be to large extent clear, up to date and self-explanatory and therefore easier to apply by PSPs.

PSPs which are PIs or EMIs (non-bank PSPs) will experience the benefits of direct participation in key payment systems and/or secure indirect access, thus enabling them to offer better and cheaper payment services to their users.

Operators of certain payment systems, those designated under SFD, whether in the public sector or private sector, will experience a one-off burden of a significant number of new applications for participation from PIs and EMIs, which will have to be processed, including full risk assessment.

1.3 Consumers and other payment service users

Payment service users will benefit from this initiative both directly and indirectly. As direct benefits, they will enjoy greater rights in the area of information concerning fees for specific transactions and estimated execution times, and improvements as regards blockage of funds (see Annex 10). Another direct benefit will be the generalised availability of IBAN verification services for all credit transfers, not only instant payments, and the resulting reduction of fraud losses.

The measures to improve enforcement and implementation of the payments rules will increase the level of protection of consumers and other users, who can be more confident that PSPs adhere to the EU rules and that measures including penalties are imposed by NCAs in cases of breaches.

Indirect benefits for users will include a wider range of competitively-priced payment services, including better account services from PIs and EMIs and improved Open Banking account information and payment initiation services. For Open Banking market research already predicts

Consumers will benefit from the possibility to obtain cash in shops without making a purchase, though this is not a right and will depend on the willingness of the shopkeeper and the availability of cash (see Annex 9).

Consumers with disabilities and other challenges to use SCA will enjoy greater financial inclusion as a result of the measure to facilitate their use of SCA described in Annex 10.

There are no specific direct costs for users associated with this initiative, other than possible fees for IBAN verification services (which will be optional for users). Competitive forces between banks and other ASPSPs should prevent any increases in general account fees.

1.4 SMEs

SMEs are concerned by this initiative in two capacities, as users of payment services (such as merchants or business users) and as PSPs, including payment fintechs (smaller PSPs, start-ups etc.). They are thus on both the supply and demand side of the payments market.

Benefits for SMEs as merchants and other corporate users of payment systems will be the same as those for users identified in the section above.

SMEs which are PSPs or payment fintechs (Open Banking TPPs or else PIs/EMIs offering payment account services) will experience the benefits for those categories noted above.

It should be noted that implementation costs for ASPSPs which are SMEs (for example for IBAN verification or for implementing an API for data access) are often lower than for larger PSPs, since larger PSPs often have a complex internal structure (e.g. resulting from mergers) or old legacy IT systems, which can significantly increase implementation costs and require ad hoc solutions. Smaller, more modern or simpler PSPs can often buy in off-the-shelf IT solutions.

Overall, SMEs are expected to be among the net gainers from this initiative, whether as users of payment services (non-financial SMEs) or as PSPs/Open Banking TPPs. Many PIs/EMIs are SMEs, and will benefit from direct access to payment systems; many Open Banking TPPs are SMEs and will benefit from an increased and better defined dataset with mandatory access. Most costs will fall on banks, and relatively few banks are SMEs.

SMEs - in both capacities as PSPs and users - will moreover benefit as will all actors in the payment market from a detailed and coherent set of rules on payments which will be applied in a coherent way across the EU, e.g. regarding criteria for penalties.

For further details about impact on SMEs, see Annex 13.

1.5 Public authorities

National competent authorities will need to devote more resources to enforcement of PSD as a result of this initiative, with potential extra staff costs as a result, although some NCAs may be able to improve PSD enforcement within current staffing levels. This will especially be the case as regards Open Banking, as each NCA will need a specialised enforcement team with knowledge in the area of APIs. This could cost in the hundreds of thousands of euro per year per NCA, which can be offset with charges to PSPs for specific services (licensing, authorisations, derogations etc.).

NCAs will furthermore benefit from a detailed and coherent set of rules on payments which will lead to easier and more cost-effective implementation of the rules.

Public authorities should benefit from improved payment services in their capacity of payment system users.

1.6 Geographical dimension of impact

The requirement to offer an IBAN verification service will proportionately have a greater cost in non-euro area Member States, since in those Member States there are fewer PSPs offering euro instant payments, and therefore fewer PSPs which have already incurred the cost of implementing IBAN verification, in line with the Commission legislative proposal on euro IPs. No other specific elements regarding the geographical impact have been identified.

2. SUMMARY OF COSTS AND BENEFITS

The tables below summarise the costs and benefits described above, based on the package of preferred options.

I. Overview of Benefits (total for all provisions) – Preferred Option		
Description	***Amount***	***Comments***
Direct benefits		
Reduction of payment fraud	The combined effect of the proposed anti-fraud measures can be anticipated as a reduction of a few percentage points in APP fraud (for example, a 10% reduction would represent €32 million of benefit annually). Wider use of SCA will also contribute to a reduction in all payment fraud.	The value of APP fraud in 2020 for all SEPA euro credit transfers in the EU is estimated by Commission services on the basis of EBA data at approximately € 323 million.
Better legal framework for Open Banking	The proposed changes are intended to support further growth of the OB sector in addition to the projected growth with no legislative change (baseline). Assuming the changes can increase the existing growth trend of Open Banking by, for example, 10%, it would create an additional €2 bn of OB market value by end 2027.	Various market research projects OB will grow. Some research explicitly include legislative changes in their predication, others do not. Taking these reports as a baseline, the EU OB users would grow from 15.5 mln users end 2021 to about 60 mln end 2024 and 80 mln end 2027. OB market value is estimated to increase from €5.5 bn end of 2021 to €11 bn end 2024 and €20.5 bn end 2027. With TPPs reported to have made additional revenues (recurring) of €1.9 bn for 2021 (35% of €5.5 bn, based on €1.6 revenues reported for 2020). Cumulative OB benefits, using the same assumptions as for users and market value, is estimated to be around 12 bn € end of 2024 and 30 bn € by 2027. See also chapter 7.2
Fairer competition between banks and non-bank PSPs	Many PIs and EMIs will be able to offer credit transfers, including instant payments, to customers for the first time.	

Better enforcement and harmonised application of PSD2	Difficult to quantify. Qualitative benefits will include: • A detailed and coherent set of rules for entities subject to EU payments legislation • Further removal of fragmentation including of gold-plating in the Internal Market • Lower compliance costs over time (as the EU payments legislation is to large extent clear, up to date and self-explaining and therefore easy to apply) • Higher legal certainty • Reduction in waiting time for action by PSPs with complaints to NCAs.	This topic combines the measures discussed in the main impact assessment under "improvement of enforcement and implementation" and also the technical clarifications described in Annex 7.
Greater consumer rights and information	Greater level of reimbursement from ASPSPs for fraudulent authorised transactions, up to €1 bn EU-wide.	See Annex 10
Merger of regimes for Payment Institutions and E-money Institutions	Administrative cost savings for PIs and EMIs	These two regimes will be combined and simplified (see Annex 8)
Indirect benefits		
A wider range of better priced payment services available	Not quantifiable	In particular, new OB services and new services from PIs and EMIs
Reduced costs for PSP of fraud complaints handling	Not quantifiable	
Reduced complaints for NCAs to handle	Not quantifiable	

II. Overview of costs – Preferred option				*II. Overview of costs – Preferred option*			
		Citizens/Consumers		Businesses[166]		Administrations	
		One-off	Recurrent	One-off	Recurrent	One-off	Recurrent
Fraud reduction	Direct adjustment costs	None	Possible fees as users of the IBAN verification service	*IBAN verification:* for those PSPs not already obliged to offer this service, about 1200-1300 in number, a total implementation cost of the order of €50m (see section 6.1.c)). The IBAN verification required for euro instant payments can be significantly leveraged to reduce implementation cost	*IBAN verification:* for those PSPs not already obliged to offer this service, costs off a few thousand euro per year (assuming a model with no charging by a service provider per check). Possibility to recover some costs from customer fees. Costs of exchanging data on fraud (voluntary)	None	Possible fees as users of the IBAN verification service
	Indirect costs	None	None	None	ASPSPs: possible compensation to payers in cases where IBAN/name check failed and in case of impersonation fraud (up to €1bn)	None	None
	Enforcement cost	None	None	None	None	None	None

[166] This category includes both business users of IPs and the PSPs.

Improvements to user rights	Direct adjustment costs	None	None	None	Min. 123m €. Education campaigns for customers on their rights/ obligations, improving financial literacy, and alerting on fraud schemes. Cost based on the VVA/CEPS' study estimates for ASPSPs.	None	None
	Indirect costs	None	None	None	None	None	None
	Enforcement cost	None	None	None	None	None	Cost of complaints handling for NCAs
Open Banking improvements	Direct adjustment costs	None	None	For some ASPSPs, cost of upgrading OB APIs or of creating new dedicated interfaces where there is none (options 2a+2d), estimated at €190 ml net. For all ASPSPs, cost of creating permissions dashboards, total cost from €12ml to €48ml For TPPs, total cost of adapting to API changes up to €26 ml, offset by savings from better APIs and no fallback	Any maintenance costs of a dedicated interface should be offset by the fact that a fallback interface is no longer required Limited maintenance cost of permissions dashboards	None	None

	Indirect costs	None	None	None	None	None	None
	Enforcement cost	None	None	None	None	None	Cost of complaints handling for NCAs
Better enforcement and application in Member States	Direct adjustment costs	None	None	None	In some cases, higher penalties for breaches	Adjustment costs of familiarisation with new rules (for example Open banking), and recruitment of extra staff in some cases	Enforcement of compliance; costs for NCAs for human resources e.g. for maintaining specialised teams supervising the various clarified provisions on open banking and fraud prevention, possibly offset by fees levied to the supervised entities. Possible 10% rise in cost of supervision (estimated by the VVA/CEPS study about €28m/€30m per year EU-wide)
	Indirect costs	None	None	None	None	None	None
	Enforcement cost	None	None	See above	None	See above	See above
Non-bank PSP access to payment systems	Direct adjustment costs	None	None	For payment system operators, cost of risk assessment and admission procedure for PIs and EMIs	For payment system operators, ongoing monitoring of new participants	For central banks as payment system operators, cost of risk assessment and admission procedure for PIs and EMIs	For central banks as payment system operators, ongoing monitoring of new participants

	Indirect costs	None	None	None	None	None	None
	Enforcement cost	None	None	None	None	None	For NCAs, cost of enforcement
Costs related to the 'one in, one out' approach							
Total	Administrative costs (for offsetting)	None	None	None	None		

3. RELEVANT SUSTAINABLE DEVELOPMENT GOALS

III. Overview of relevant Sustainable Development Goals – Preferred Option(s)		
Relevant SDG	**Expected progress towards the Goal**	**Comments**
Target 8.2 of the UN Sustainability Development Goals: "To achieve higher levels of economic productivity through diversification, technological upgrading and innovation, including through a focus on high-value added and labour-intensive sectors"	Improved functioning of payment systems and better payment services.	

ANNEX 4: ANALYTICAL METHODS

To adequately assess the impact of this proposal, this report builds on the analysis of the following sources of data:

1) The Commission's stakeholder consultation strategy, as outlined in Annex 2;
2) A study carried out by a consortium composed of VVA Brussels SPRL and the Centre for European Policy Studies (CEPS) with the support of the Nicolaus Copernicus University in Toruń.
3) EBA's Advice in response to the Call for Advice on a number of specific topics related to the impact and application of specific areas of the PSD2. Response to the Call for Advice was based on input received from NCAs.

This Annex outlines the analytical framework and methods employed in the collection and analysis of data within the scope of each of the above components.

1. The Commission's stakeholder consultation strategy

To ensure that views of different stakeholders were adequately taken into account in the impact assessment, a stakeholder consultation plan was adopted that comprised the following components, and of which the findings have been described in Annex 2.

Data collected via the various consultations informed both quantitative and qualitative analysis. Quantitative insights were drawn by deploying a) the clustering and summary tools available in the DORIS consultation dashboard, b) frequency analysis of answers to closed questions elicited through the public consultation, and c) the cost- benefit analysis (*cf. Annex 3*).

Qualitative analysis focused on responses to open-ended questions elicited through the public consultation, as well as minutes and reports from thematic sub-groups in Payment Systems Market Expert Group (PSMEG) meetings, as well as the ad-hoc bilateral stakeholder meetings. More precisely, with regard to contributions to open-ended questions in the targeted consultation, responses were analysed and coded attending to a) key topics and/views (e.g. customer protection, enforcement, open banking), as well as b) the distinct type of stakeholder (e.g. Competent Authority, ASPSPs, TPPs, consumer organizations).

Finally, insights from both quantitative and qualitative analysis were systematically brought together according to frameworks and tools prescribed in the Better Regulation Guidelines and Toolbox.

2. The VVA/CEPS study

This study was based on desk-based research, fieldwork, and analysis. The consultation activities included 8 scoping interviews, 232 stakeholder interviews, an online survey with 65 responses and 13 follow-up interviews. The study was prepared in accordance with the Better Regulation Guidelines and Toolbox.The study comprises three tasks, namely: i) Desk-based research; ii) Fieldwork; and iii) analysis.

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.

The aim of Task 2 was to collect all the necessary legal and primary evidence to respond to the evaluation questions. In this regard, national legal experts conducted legal desk research in ten selected Member States, namely Belgium, France, Germany, Ireland, Italy, Lithuania, the Netherlands, Poland, Spain and Sweden.

The aim of the in-depth fieldwork was to gain a comprehensive picture of different views and perspectives on the study questions. The stakeholder consultation envisaged under the study aimed to collect both qualitative and quantitative data, to assess the implementation and application of the Directive (EU) 2015/2366 on Payment Services (PSD2). The consultation activities were varied and designed in a way to target a wide range of stakeholders through a series of key activities, using multiple tools and channels, in order to gather insights from as many relevant views as possible. The consultation activities included:

i. Scoping interviews (January 2022)
ii. Stakeholder interviews (16 March to 11 July 2022)
iii. Online survey (21 March to 15 July 2022)
iv. Follow-up interviews (21 March to 15 July 2022)

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). Further details on the participation of the different stakeholders in the different consultation activities in the study are provided in Annex I of the study[167].

i. Scoping interviews

The objective of the scoping interviews was to gather as much first-hand experience, with as many details as possible from various stakeholder groups. Throughout the month of January 2022, eight scoping interviews were carried out. These were primarily with EU associations Payment Service Providers (PSPs) and a consumer association. The interviews were performed in a semi-structured format to encourage two-way communication to raise awareness of the study and obtain stakeholders' contact details for further phases of the study.

[167] The VVA/CEPS study can be accessed here, and its Annexes can be accessed here.

The scoping interviews allowed to further define data needs, impact identification, stakeholder mapping[168] and other questions related to the methodology development based on the stakeholders' experience in the field. The interviews provided qualitative data on key aspects to better understand the challenges linked to the PSD2, as well as areas for its improvement.

ii. Stakeholder interviews

The aim of the stakeholder interviews was to:

1. Gather legal and economic evidence on the application and impact of the PSD2 on the payments market and on any benefits and challenges which may have arisen from PSD2;
2. Where modifications to PSD2 might be considered appropriate, in particular in the context of a possible proposal to revise PSD2.

As a result, the information collected during the interviews contributed to the review of PSD2 by assessing its effectiveness, efficiency, relevance, coherence with other legislative acts, and EU value-added. It provided to the research team an **insight concerning the difficulties of implementing the Directive and allowed to verify findings of the legal desk research**. The Member States where the implementation of the Directive triggered issues and difficulties, and the interviews with National Competent Authorities (NCAs) confirmed why this is the case and how it affects the validity of data collected in these countries for the evaluation indicators. In order to reflect the different requirements and to have a better understanding of each stakeholder's position and experience with the Directive, stakeholder-specific questionnaires were produced. In this way, the interviews covered all relevant issues and gave the flexibility for interviewees to go into greater depth on issues where the interviewees are particularly knowledgeable. The interviewees also had the possibility to send their replies in written form, as well as to provide the study team with any documentation deemed useful for the purposes of the study. The questionnaires were oriented to a large extent around the questions indicated in the Terms of Reference, along with the insights gathered in the scoping interviews, desk research and literature review. Seven different types of questionnaires were designed for different types of stakeholders (Cf. Annex I of the VVA/CEPS study).

iii. Survey

In terms of content, the survey covered the questions from the Terms of Reference, as well as insights gathered from scoping interviews. Once the survey design had been finalised, the first few invitations were taken into account as a pilot. Through this approach, the research team had the opportunity to adjust and edit the questionnaire where necessary. The analysis on the survey responses helped to shed light on the evaluation questions to be addressed (i.e. relevance, effectiveness, efficiency, EU added value and coherence) and to complement the interviews, especially in the countries that were not among the focus countries. The survey thus allowed to complete and triangulate the results of the interviews.

[168] It enabled the research team to take into consideration a range of stakeholders. This includes, NCAs, National ministries, consumer associations, payment service providers i.e banks, TPPs etc (both big and small market players), Payment service users (of both big and small merchants)

iv. Follow-up interviews

The last step in the data collection was to carry out follow-up interviews in the 10 focus Member States. A total of **13 stakeholders** provided replies to the survey, which was targeting National Competent Authorities (Ministries of Finance, Economics, Justice and Supervisory Authorities); EU and National associations; Payment Service Providers (e.g., banks, payment institutions) and Payment Services Users (i.e. consumer associations and merchants)**.**

The follow-up interviews were aimed at gaining deeper qualitative insight on the functioning of the Directive. These interviews were conducted following the same questionnaire as the one conceived for the main interviews, while applying a more semi-structured approach. This gave the flexibility to stakeholders to go into greater depth on issues where the interviewee had particular knowledge on. The qualitative assessment from interviews and desk research was cross-analysed with quantitative information collected as part of CBA.

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 are briefly described below.

- ***Step 1: Definition of scope and methods***

As a first step, the analysis began with the identification of the key cost and benefit items to be assessed, as well as the related data sources and assumptions to be made. Next, a typology was created based on an assessment of two dimensions, namely (1) the identification of affected stakeholders and (2) the classification of potential costs and benefits that accrue to each of these stakeholder groups.

- ***Step 2: Data collection***

The main tools for collecting information for the CBA were developed as part of the stakeholder consultation, namely the questionnaires for interviews with actors on the payments market. The semi-structured nature of the interviews made it possible to obtain some quantitative information (either during the discussion or in the follow-up), while the questionnaire contained explicitly quantitative questions. The work undertaken for the literature review, especially the input from surveys, interviews and data sources, was critical for the estimation of the costs and benefits.

Additional data required to conduct the CBA was obtained from several sources. Data on the number of relevant stakeholders was downloaded from the EBA's Credit Institution and payment and E-Money Institutions registers[169] and was combined with Orbis data for size, turnover and earnings before interest and taxes (EBIT) figures. The affected TPP population was derived from three categories, namely E-Money Institutions, payment institutions and AISPs with code values PS_070 (Payment initiation services) and PS_080 (Account information services), yielding 189 TPPs in the EU, with 151 registered after PSD2

[169] The definition used for TPPs is more restrictive (i.e. excludes exempted entities) than reported under some other sources. Therefore the overall costs and benefits for these entities could be higher.

transposition in 2018. These values are generally lower than what is reported in the literature. This is because the definition applied here does not include exempted TPPs (PSD_EPI and PSD_EEMI). Data from the Orbis database was used to classify TPPs by size (in terms of employees[170] – micro (<10) and other undertakings (>10). This was necessary because of assumptions derived from interviews and the survey.
As there is no publicly available source indicating payment institution registration fees for all EU countries, where available, registration costs were collected from diverse online sources. For the rest, an unweighted average of the countries for which the registration fees were available was applied.

Regarding credit institutions, it is assumed that credit institutions active in corporate groups and/or networks have some scale advantages in the implementation of the requirements. The number of banking groups/networks was identified by using the criterion of at least € 30bn in turnover to make their number comparable to that of significant supervised entities under the SSM for each country (which, besides this threshold, are also selected based on additional criteria not considered here).

Payment data, in particular on card transactions, credit transfers and number of POS terminals came from ECB statistics[171]. EU-wide API call information is based on Konsentus estimates[172], while some ASPSPs provided data on API calls recorded. This information was used for the extrapolation of API maintenance costs. E-commerce data was estimated based on EuroCommerce reports[173]. Data on fraud rates related to SCA and non-SCA authenticated payments are based on the EBA's preliminary observations[174]. Finally, labour costs are estimated based on data available on Eurostat. The data was used to calculate daily labour costs for finance/insurance activities and public administration in each country, as well as an EU average. As per the recommendation of the Better Regulation Toolbox (# 58), the labour costs were increased by 25% to reflect overhead cost.

- ***Step 3 - Analysis and triangulation of data***

The third step of the CBA consisted of the data analysis, which was split into two parts:

1. a qualitative analysis, based on semi-structured stakeholder interviews and qualitative findings from desk research,
2. a quantitative analysis, based on the questionnaire and data available online, complemented with interviews and quantitative findings from desk research.

The methodology for estimating costs and benefits varies across the typology. The majority of costs were estimated through the Standard Cost Model (SCM, as detailed below), and in accordance with the Better Regulation Toolbox (# 58). To meet the proportionality principle, obligations with a clearly marginal aggregated economic impact did not undergo a full-fledged SCM-based quantification. Instead, they are subject to a simplified assessment, focused on the stakeholders that would be most affected in relative terms.

---

[170] See defintions here
[171] Report available here. Data used includes credit transfer, card payment, e-commerce volume and value.
[172] See TPP tracker.
[173] See 2022 report here.
[174] See here.

The quantitative CBA data was assessed in a disaggregated form for each Member State to allow for a comparison and assessment of potential correlations between costs/benefits. The formulas used in calculating the actual administrative costs allow to weigh direct and indirect costs and benefits, based on size and type of businesses/stakeholders assessed. Annex 8 of the VVA/CEPS study provides further detail on the assumptions and formulas for the calculation of the different cost and benefit items estimated by the evaluation.

- ***Step 4 - Revision and finalisation of findings***

The last step of the CBA consisted of the development of the cost-benefit analysis output. The CBA findings were circulated across the senior members of the project team, discussed in a peer-review format, and were tested and finalised.

2. EBA Advice

On 20 October 2021, the Commission submitted to the EBA a Call for Advice regarding the review of PSD2. The objective of the Cal for Advice was to gather evidence on the application and impact of PSD2, including any benefits and challenges that may have arisen with regard to the implementation and application of the Directive. Moreover, the Commission invited the EBA, based on the experience and EBA's mandate, to identify areas where amendments to the PSD2 might be appropriate. The EBA was invited to deliver the report by 30 June 2022. The scope of the Call for Advice comprised 28 questions under the following nine sections:

a. Scope and definitions;
b. Licensing of PIs and supervision of PSPs under PSD2;
c. Transparency of conditions and information requirements;
d. Rights and obligations;
e. Strong customer authentication;
f. Access to and use of payment accounts data in relation to AIS and PIS;
g. Access to payment systems and accounts maintained with a credit institution;
h. Cross-sectoral topics;
i. Enforcement of PSD2.

The EBA decided to follow a methodological approach whereby the EBA first identified the most significant and controversial issues related to the interpretation and application of the legal requirements of PSD2 and the EBA legal instruments within the scope of each question posed in the Call for Advice. Second, the EBA collected feedback from CAs on these issues, together with the proposed solutions on how to address them. Finally, the EBA assessed the feedback received, discussed it with the CAs and agreed on the response to each question.

The EBA also leveraged on the experience accrued during the development and monitoring of the application of the EBA legal instruments under PSD2 and the additional own-initiative Guidelines, as well as the clarifications provided through a number of EBA Opinions and more than 200 answers to questions posed in the EBA Q&A tool.

ANNEX 5: EVALUATION REPORT

TABLE OF CONTENTS

1. INTRODUCTION 99
- 1.1 Purpose of the PSD2 evaluation 99
- 1.2 Scope of the PSD2 evaluation 100
- 1.3 Description of the methodology 100
- 1.4 Limitations and robustness of the methodology 101

2.WHAT WAS THE EXPECTED OUTCOME OF THE INTERVENTION? 102
- 2.1 Description of the intervention and its objectives 102
- 2.2 Point(s) of comparison 105

3.HOW HAS THE SITUATION EVOLVED OVER THE EVALUATION PERIOD? 106
- 3.1 Implementation of PSD2 106
- 3.2 Description of current situation 99

4. EVALUATION FINDINGS (ANALYTICAL PART) 118
- 4.1 To what extent was the intervention successful and why? 118
- 4.1.1 Effectiveness 118
- 4.1.2 Efficiency 134
- 4.1.3 Coherence 138
- 4.1.3.1 Internal coherence 138
- 4.1.3.2 External coherence 139
- 4.2 How did the EU intervention make a difference and to whom? 143
- 4.3 Is the intervention still relevant? 145

5. WHAT ARE THE CONCLUSIONS AND LESSONS LEARNED? 156
- 5.1. Conclusions 157
- 5.2. Lessons learned 159

1. INTRODUCTION

The revised Payment Services Directive[175] (PSD2 – Directive (EU) 2015/2366) adopted in 2015 aims to develop a competitive and innovative single market for payment services with a high level of security and protection for consumers and businesses by improving the previous rules (PSD1). In particular, the Directive aims to:

- make it easier and safer to use online payment services;
- better protect payment services users against fraud, abuse, and payment problems;
- promote innovative payment services;
- strengthen the rights of payment services users.

Most of the provisions in PSD2 have been applicable since January 2018, but some provisions on strong customer authentication (SCA) and access to payment accounts data apply since September 2019.

1.1 Purpose of the PSD2 evaluation

This evaluation differs from the review report foreseen by PSD2, whose Article 108 requires the Commission to report on the application and impact of the Directive by 13 January 2021[176], in particular with regard to the rules on charges, the scope of application, certain thresholds, the access to payment systems and the introduction of maximum limits for the amounts to be blocked on the payer's payment account. Furthermore, the review clause mandates the Commission to submit a legislative proposal, if appropriate. The review report will be published together with the revision of PSD2.

The PSD2 evaluation presented in this document is retrospective. It has been conducted for the purpose of and in parallel ('back-to-back') with the impact assessment accompanying the proposal revising PSD2. The results of this evaluation have been incorporated in the problem definition of the impact assessment.

The evaluation covers the period from the application of the PSD2 (13 January 2018) until end 2022. In line with the Better Regulation Toolbox[177], it examines whether the objectives of the Directive were met during the period of its application (*effectiveness*) and continue to be appropriate (*relevance*) and whether the PSD2, taking account of the costs and benefits associated with applying it, was efficient in achieving its objectives (*efficiency*). The evaluation also considers whether the Directive, as legislation at EU level, provided added value (*EU added value*) and is consistent with other related pieces of legislation (*coherence*).

---

[175] 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 (OJ L 337, 23.12.2015, p. 35–127).

[176] This review could not take place by the date provided for in the Directive due to its late transposition by some Member States and the delay in applying some of its rules.

[177] European Commission (2021) Better Regulation Toolbox, Chapter 6, Tool #47.

This evaluation is part of the general PSD2 review process, announced in the Digital Finance Strategy[178], the Retail Payments Strategy[179] and the 2023 Commission work programme[180].

1.2 Scope of the PSD2 evaluation

The scope of the present evaluation includes the PSD2 in its entirety.

The Directive is accompanied by a number of Delegated and Implementing Acts and further guidance in the form of Guidelines, Opinions and more than 200 Q&As provided by the European Banking Authority (EBA). Related delegated and/or implementing acts were not assessed on a standalone basis.

The geographical scope of the evaluation extends to all EU Member States. By virtue of Article 288 TFEU the Directive is binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods. PSD2 is of EEA relevance and was incorporated into the EEA Agreement. However, the evaluation does not extend to Iceland, Liechtenstein and Norway.

1.3 Description of the methodology

The evaluation, being part of the general review process of the Directive, was supported by a study carried out by an external contractor, a Consortium composed of VVA Brussels SPRL (lead) and the Centre for European Policy Studies (CEPS) with the support of the Nicolaus Copernicus University in Toruń. The final 'Study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2)'[181] (hereafter 'the VVA/CEPS study'), which was delivered to the Commission on 7 October 2022, provides a comprehensive assessment of the application and impact of PSD2 and is based on three methodological approaches: desk-based research, fieldwork, and analysis. The consultation activities included 8 scoping interviews, 232 stakeholder interviews, an online survey with 65 responses and 13 follow-up interviews. The study was prepared in accordance with the Better Regulation Guidelines and Toolbox.

The evaluation also builds on feedback received (195 responses) in the context of the Call for Evidence (see Annex 2).

---

[178] Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions On A Digital Finance Strategy For The EU, COM(2020) 591 final, 24.9.2020.

[179] 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, 24.9.2020.

[180] Annexes To The Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions, Commission work programme 2023, COM(2022) 548 final, 18.10.2022.

[181] FISMA/2021/OP/0002, A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2). Available here.

A public consultation on the PSD2 review was organised on the 'Have your say'-website (hereafter 'the public consultation'), which ran between 10 May and 2 August 2022 and received 101 responses. This consultation includes questions for a broader audience that does not necessarily possess specific knowledge of payment services. In parallel, a separate targeted public consultation (hereafter 'the targeted consultation') ran between 10 May and 5 July 2022 and gathered input from professional stakeholders such as payment service providers, national- and EU authorities and regulators or payment experts. The targeted consultation attracted 169 responses. See Annex 2 for further details on these consultations.

On 20 October 2021, DG FISMA sent a Call for Advice to the EBA on a number of specific topics related to the impact and application of specific areas of the PSD2. These topics include (i) the scope and definitions of PSD2, (ii) authorisation, supervision and enforcement, (iii) transparency of conditions and information requirements, (iv) rights and obligations, (v) SCA, (vi) access to and use of payment accounts data in relation to payment initiation services and account information services, (vii) access to accounts of payment institutions maintained with a credit institution and (viii) cross-sectoral topics. On 23 June 2022, the EBA published an 'Opinion on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2)'[182] in response to the Call for Advice (hereafter 'the EBA Advice').

These topics were also discussed in two dedicated meetings with Member States in the Commission Expert Group on Banking, Payments and Insurance (CEGBPI) on 30 November 2021 and 7 April 2022, completed by written contributions from the experts. The Payment Systems Market Expert Group (PSMEG) was also consulted in three meetings on 16 December 2021, 5 April 2022 and 3 October 2022 and its members provided comprehensive written input[183].

In addition, the involvement of stakeholders took place through a large number of bilateral meetings with numerous stakeholders.

1.4 Limitations and robustness of the methodology

The efficiency analysis presented in the VVA/CEPS study is based on the results of the cost-benefit analysis and stakeholder consultation as well as an analysis of the relevant literature[184]. 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

---

[182] European Banking Authority (EBA/Op/2022/06) Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2), of 23 June 2022.

[183] The PSMEG consists of a maximum of 40 Members and represents in balanced proportions the payment services industry and users of payment services.

[184] VVA/CEPS study, Annex 8: Cost-benefit analysis methodological note.

effects. This is not unexpected, as these impacts are only now becoming visible due to late transposition by Member States and the late entry into force of some key provisions such as SCA. Therefore, the longer-term effects can still only be estimated. In addition, costs and benefits may vary between Member States. However, the findings from studies and more recent surveys[185] do provide an indication of the most critical aspects, which account for the bulk of the costs arising from the implementation of the Directive.

2. WHAT WAS THE EXPECTED OUTCOME OF THE INTERVENTION[186]?

2.1 Description of the intervention and its objectives

In the Commission's 2012 Communication "Single Market Act II – Together for new growth"[187], the modernisation of the legislative framework for retail payments was identified as a key priority in light of its potential for new growth and innovation. The revision of the PSD1[188] and the preparation of a legislative proposal on multilateral interchange fees for card payments[189] were defined as one of the key actions of the Commission for 2013.

PSD2 is the most comprehensive and relevant set of EU rules in the field of retail payments. It provides the legal basis for the supervision of payment institutions and defines the information requirements and the rights and obligations between payment services providers (including banks, payment institutions, and e-money institutions) and payment services users (including consumers and merchants).

PSD2 widens the scope of PSD1 for example by adding two new payment services that are based on access by third party providers (TPPs) to customer data held primarily by credit institutions, namely payment initiation services (PIS) and account information services (AIS).

PSD2 also updates the exemption for telecom operators [Article 3(l)][190] by limiting it mainly to micro-payments for digital services and includes transactions with third countries when only one of the payment service providers is located within the EU ("one-leg transactions"). It also enhances cooperation and information exchange between authorities in the context of authorisation and supervision of payment institutions. The EBA is mandated to develop a central register of authorised and registered payment institutions.

---

185 Ibid.

186 PSD2 is referred to in this Evaluation Report as "the intervention".

187 European Commission Communication "Single Market Act II - Together for new growth", COM(2012) 573 final.

188 Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market.

189 Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions.

190 PSD: frequently asked questions (point 9).

To ensure a high degree of consumer protection with regard to electronic payments, PSD2 introduces enhanced security measures to be implemented by all payment service providers, including banks. In particular, PSD2 requires payment service providers to apply SCA for electronic payment transactions as a general rule.

The proposal was published by the Commission on 24 July 2013, agreed by the co-legislators on 5 May 2015, and published in the Official Journal of the European Union on 23 December 2015. The Directive entered into force on 12 January 2016. Member States had to transpose the provisions of the Directive into their national laws and regulations by 13 January 2018.

The intervention logic includes seven 'needs', which link back to the main problems identified in the PSD2 Impact Assessment[191] before the introduction of PSD2, when PSD1 was still in force. These needs, or problems, relate to three problem drivers:

1) ***Market failures***: 1.1. a fragmented market for innovative solutions (*Need 1*), and 1.2. competition issues in some payment areas (*Need 2*);

2) ***Regulatory and supervisory gaps***: 2.1. diverse charging practices between Member States (*Need 3*), 2.2. legal vacuum for certain PSPs (*Need 4*), 2.3. the inconsistent application of PSD1 (*Need 5*), and 2.4. diverging supervisory and licencing rules and practices (*Need 6*);

3) ***Lagging consumer protection*** (*Need 7*).

The intervention logic builds on these needs and identifies five main and six specific policy objectives, as outlined in the PSD2 Impact Assessment[192]. The main objectives are:

6. To ensure a level playing field between incumbent and new providers of card, internet and mobile payments;
7. To increase the efficiency, transparency and choice of payment instruments for payment service users (consumers and merchants);
8. To facilitate the provision of card, internet and mobile payment services across borders within the EU by ensuring a Single Market for payments;
9. To create an environment which helps innovative payment services to reach a broader market;
10. To ensure a high-level protection for PSUs across all Member States of the EU.

These main objectives are supplemented by the following specific objectives:

---

[191] SWD(2013) 288 final, p. 15 et seq. Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a directive of the European parliament and of the Council on payment services in the internal market, SWD(2013) 288 final, p. 15 et seq.

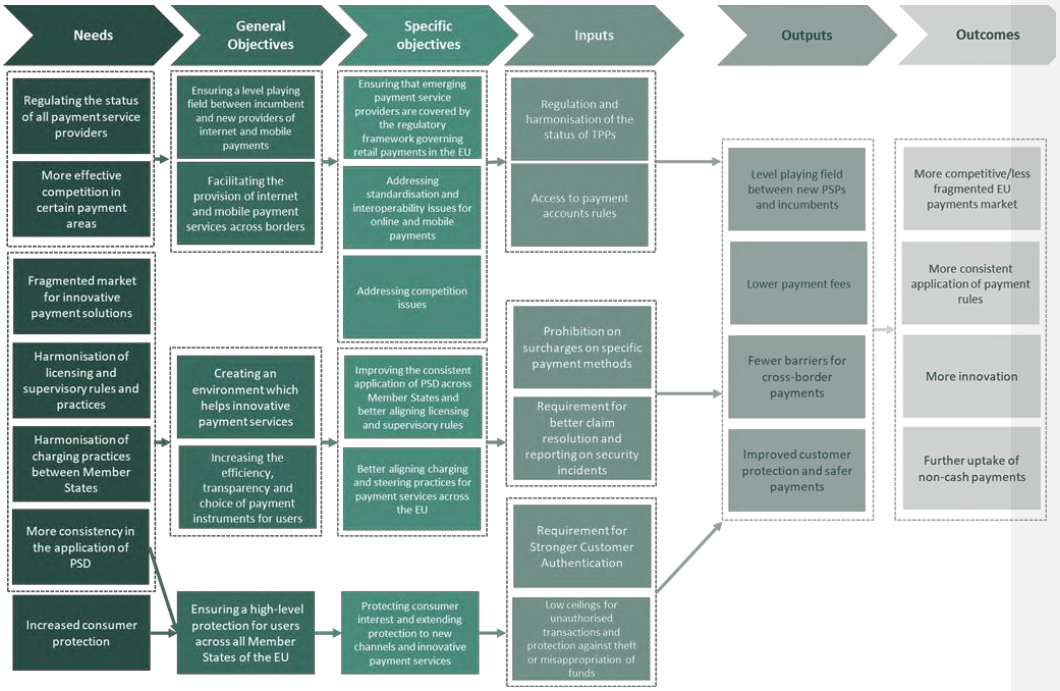
[192] Ibid., p. 35 et seq.

1. To address standardisation and interoperability gaps for card, internet and mobile payments;
2. To eliminate hurdles for competition, in particular for card and internet payments;
3. To better align charging and steering practices for payment services across the EU;
4. To ensure that emerging payment service providers are covered by the regulatory framework governing retail payments in the EU;
5. To improve the consistent application of the legislative framework (PSD1) across Member States and to better align licensing and supervisory rules for payment services across Member States;
6. To protect the consumer interests in view of regulatory changes in the card business and to extend the regulatory protection to new channels and innovative payment services.

These main and specific objectives, in turn, define the expected outputs and outcomes following the changes introduced by the PSD2. 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. 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.

In order to achieve these outputs and outcomes, the intervention logic succinctly lists a set of 'inputs', i.e. the key changes introduced by PSD2, namely: i) regulation and harmonisation of the status of TPPs, ii) laying down access to payment accounts rules, including the lawful use of consumer data, iii) prohibition of surcharges regarding specific payment methods, iv) laying down a better claim resolution and reporting on security incidents, v) laying down requirements for SCA, vi) setting low ceilings for unauthorised transactions and laying down protection against theft or misappropriation of funds.

Figure 5: Logic of the intervention



Source: VVA/CEPS study, based on the PSD2 Impact Assessment

2.2 Point(s) of comparison

The present evaluation assesses the PSD2 against the baseline under its predecessor Directive 2007/64/EC (PSD1), which was adopted in December 2007 on the basis of a Commission proposal of December 2005.

PSD1 provided the legal foundation for an EU single market for payments, to establish a harmonised legal framework supporting safer and more innovative payment services across the EU. The objective was to make cross-border payments as easy, efficient and secure as domestic payments within a Member State. Since 2007, this Directive has brought substantial benefits to the European economy, easing access for new market entrants, including payment institutions, and offering more competition and choice to consumers. By providing a harmonised set of rules for the provision of payment services in a consistent manner throughout the EU, it enabled companies to benefit from economies of scale and facilitated the operational implementation of the Single Euro Payments Area (SEPA). PSD1 brought more transparency and information for consumers, for example about fees. It increased

efficiency by for instance cutting execution times. It also strengthened refund rights and clarified the respective liability of consumers and payment service providers. A very tangible benefit was that payments were made easier and quicker throughout the whole EU: in principle, payments were credited to the payment receiver's account within the next day.

The analysis of the impact of PSD1 and the consultation on the Commission Green Paper of 11 January 2012, entitled, 'Towards an integrated European market for card, internet and mobile payments'[193], have shown that market developments have given rise to significant challenges from a regulatory perspective. As outlined in recital 4 of PSD2, "*significant areas of the payments market, in particular card, internet and mobile payments, remained fragmented along national borders. Many innovative payment products or services (such as payment initiation or account information services) did not fall, entirely or in large part, within the scope of PSD1. Furthermore, the scope of PSD1 and, in particular, its exclusions, such as certain payment-related activities (e.g. payment services provided within a "limited network" or through mobile phones or other IT devices), had proved in some cases to be too ambiguous, too general or simply outdated, taking into account market developments. This had resulted in legal uncertainty, potential security risks in the payment chain and a lack of consumer protection in certain areas. It had proven difficult for payment service providers to launch innovative, safe and easy-to-use digital payment services and to provide consumers and retailers with effective, convenient and secure payment methods in the Union*".

PSD2 was adopted to address these problems by setting out the measures identified above.

3. HOW HAS THE SITUATION EVOLVED OVER THE EVALUATION PERIOD?

3.1 Implementation of PSD2

The deadline for transposing PSD2 was 13 January 2018, whereas the deadline for the migration to SCA was 14 September 2019.

In March 2018, the Commission launched infringement procedures against 16 Member States for non-communication of transposition measures, of which 14 were closed.

To date, all Member States have notified full transposition of the Directive. The last three Member States only notified full transposition of the Directive in January and February 2020. The late transposition by Member States not only led to a postponement of the completeness and conformity assessment, but also had an unfavourable impact on the timing of the review process.

The completeness assessment was finalised in 2021. Since November 2019, informal clarification requests were sent to a total of 23 Member States. The Commission concluded

[193] European Commission, Green Paper Towards an integrated European market for card, internet and mobile payments, COM(2011) 941 final, 11.1.2012.

that the national transposition measures of 24 Member States were complete. However, completeness checks for 3 Member States are still pending.

The Commission is currently finalizing the conformity checks. In this context, informal clarification requests were sent to 20 Member States in December 2022 on the transposition of a number of PSD2 key provisions.

Since the entry into force of the Directive on 12 January 2016, the EBA has supported the implementation of the Directive through the development of seven Technical Standards[194], eight sets of Guidelines, eight Opinions, and more than 200 Q&As. While the Q&A process proved to be an efficient tool for interpreting the PSD2 legal framework, due to its non-binding nature there is no guarantee that the answers to the Q&As will be enforced in all Member States.

The implementation of the SCA provisions proved to be particularly difficult due to the challenges arising from the changes that were required, especially by actors that were not payment service providers (PSPs), such as e-merchants, which lead to some actors in the payments chain not being ready by 14 September 2019. SCA must be based on two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is), which are independent of each other. To ensure a smooth migration to SCA-compliant solutions for card-based payment transactions in internet commerce, the EBA granted on an exceptional basis supervisory flexibility for National Competent Authorities (NCAs) not to enforce the security requirements from its legal application date (on 14 September 2019), but as of 31 December 2020[195]. In return, the EBA set out actions to be taken by NCAs and affected payment services providers (PSPs), which had to report on a regular basis to NCAs on the progress made. Some industry stakeholders interviewed by VVA/CEPS reported that the overall delay in implementation of SCA, as well as the publication of additional standards and multiple opinions by EBA created legal uncertainty, complexity and implementation challenges[196].

3.2 Description of current situation

Since the adoption of PSD2, new players and new services have emerged in the retail payments market. More specialised non-bank providers (payment fintechs) have entered the market and provide newly regulated services (account information and payment initiation). Large technology companies have extended their activities into the payments domain. Big

---

[194] Regulatory Technical Standards on Home-Host cooperation under PSD2; Regulatory and Implementing Technical Standards on the EBA Register under PSD2; Regulatory Technical Standards on central contact points under PSD2; Regulatory Technical Standards on passporting under PSD2; Regulatory Technical Standards on strong customer authentication and secure communication under PSD2; and Regulatory Technical Standards on payment card schemes and processing entities under the IFR.

[195] European Banking Authority (EBA-Op-2019-11) Opinion of the European Banking Authority on the deadline for the migration to SCA for e-commerce card-based payment transactions, of October 2019.

[196] VVA/CEPS study, p. 137.

hybrid groups have emerged, providing both PSD2-regulated and non-regulated services such as payment processing. New types of digital payment solutions, such as those based on e-money, on digital wallets or on traditional payment instruments such as cards are increasingly popular. Crypto-assets and stablecoins have appeared in the payments landscape.

This entry of new players has occurred in a context where the retail payments market[197] has been undergoing key changes largely related to the increasing use of cards and other electronic payment methods. Compared with 2018, when PSD2 entered into force, the total number of non-cash payments in the EU, comprising all types of payment services, increased by 2.5% in 2021 to 143.2 bn, despite the total value decrease by 15% to EUR 239.9 trillion. Payment cards are the most popular means of cashless payments in terms of number of transactions (Figure 3). In 2021, card payments represented 52% of all cashless transactions in the EU, although this share has decreased since 2018 (when card payments constituted 55.5% of all cashless payments)[198].

Figure 6: Cashless payments in billion (EU)

	2015	2016	2017	2018	2019	2020	2021
Total number (bn)	114.3	123.2	128.1	139.7	152.0	126.9	143.2
Total value (tn)	276.7	281.4	289.3	282.8	290.3	202.0	239.9

Source: ECB Statistical Data Warehouse; figures are for EU (changing composition); Value figures are for all currencies combined - denominated in Euro

While focusing on the euro area only, the ECB's 2022 study on the payment attitudes of consumers in the euro area (SPACE)[199] offers more nuanced insights. Notably, it shows that, while cash (banknotes and coins) remains the most used means of payment at POS and P2P proximity payments (both in terms of number and value), its share in overall turnover has been declining. Accordingly, in 2022, cash was used in 59% of POS transactions in the euro area, significantly down from 72% in 2019[200] and 79% in 2016[201]. More precisely, cash remains most frequently used for small value payments at the POS, in line with the previous

[197] Retail payments designate payment services used by non-MFIs (monetary and financial institutions), including cards, credit transfers, direct debits, e-money and cheques.

[198] ECB Statistical Data Warehouse. Figures designate cards issued by resident PSPs, all cards except e-money function.

[199] ECB's 2022 Study on the payment attitudes of consumers in the euro area (SPACE) builds on data collected through a survey of a random sample of the population in all euro area countries. It follows an identical SPACE from 2020 and 2016 study on the use of cash by households in the euro area (SUCH).

[200] Data from the 2020 Study on the payment attitudes of consumers in the euro area (SPACE)

[201] Data from the 2017 survey on the use of cash by households (SUCH).

studies whereas for payments over EUR 50 cards were the most frequently used method. Most noticeably, although cards were used in 34% of POS transactions (up from 25% in 2019 and 19% in 2016), in terms of value of payments, they accounted for a higher share of transactions than cash (46% compared to 42%). This contrasts with 2019 and 2016, when cash payments accounted for a higher share of value of payments than card transactions (47% compared to 43% in 2019 and 54% compared to 39% in 2016).

According to the same report, this trend of increase of cashless payments is also found in P2P (proximity) payments. In 2022, while cash remained the dominant means of payment in person-to-person (P2P) transactions in the euro area, its share in the total number of payments declined from 86% in 2019 to 73% in 2022 (from 65% to 59% in terms of value). In contrast, cashless means of payments have increased in P2P payments between 2019 and 2022. Particularly, the share of payments using mobile phone apps more than tripled in terms of number during this period from 3% to 10%, and in terms of value, from 4% to 11%.

This evolution towards cashless payments does not materialize evenly across all EU. For instance, the share of card payments is well above 52% in Portugal (72.2%) and Romania (71.8%), where it has not changed significantly compared to 2017. In contrast, the use of cards is also below the EU average in Germany (30.3%) and Bulgaria (35%), although in both cases these figures represent an increase of about 10p.p when compared to 2017. Moreover, the trend towards cashless payments has not only been characterized by an increase in card payments, but also by the increasing uptake of e-money payments (5.2% of overall transactions in the EU in 2021 compared with 3.3% in 2017). However, here too staggering differences can be found across Member States. Indeed, Luxembourg stands out, with the highest number of e-money transactions (5 billion in 2021, representing a 93.3% share of all transactions in 2021), while e-money payments also have a higher relative importance than the EU average (5.2%) in Italy (15.7%), Ireland (11.7%) and Malta (11.6%). In contrast, this instrument has gained comparatively little traction in the Netherlands (0%), Austria (0.2%) and France (0.2%), as well as in non-Euro Member States Denmark (0.1%) and Sweden (0%)[202].

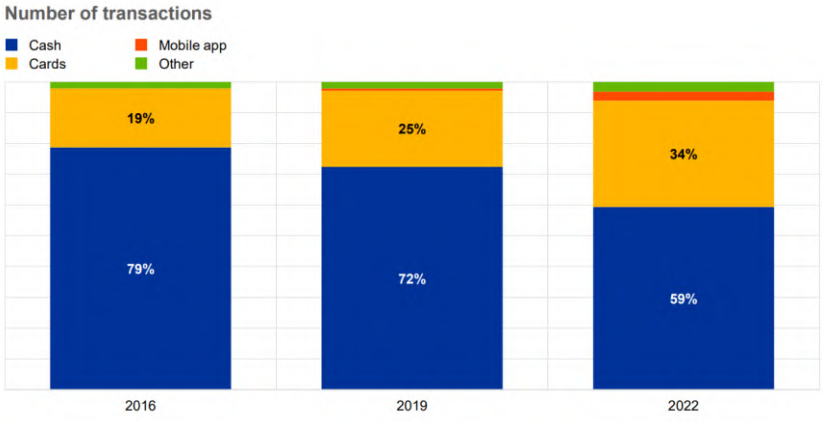
Among cashless payments, some developments have been identified with regard to contactless cards, mobile wallets and instant payments. The most used contactless payment solutions in the EU are NFC-based, while other technologies such as QR (Quick Response) codes, are also slowly gaining traction. In particular, contactless card payments at the POS increased significantly in three years, from 41% of all card payments in 2019 to 62% in 2022. Regarding mobile payments, while consumers are making payments using mobile phone apps more often than before, their share in total POS payments in 2022 was still relatively low compared to cash and card payments. Accordingly, mobile payments accounted for 3% of the number of transactions in 2022 (up from 1% in 2019) and 4% of the value (up from 1%).

---

202 ECB, Statistical Data Warehouse, Payment statistics report, July 2022.

Also, digital wallets are becoming popular at point of sale. In 2021, mobile wallets[203] accounted for 7.7% of POS value spent in the EU[204].

Figure 7: Share of payment instruments used at the POS in terms of number of transactions, 2016-2022, euro area

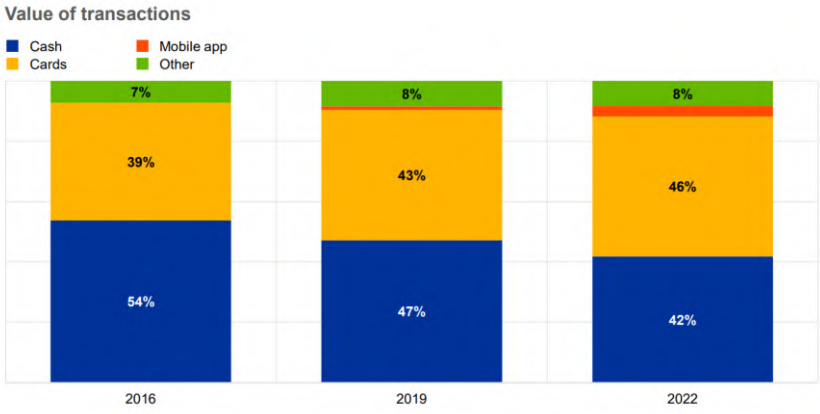


Source: ECB 2022 SPACE

[203] Wallets can be funded directly via cash, cards, bank transfer or other methods like cryptocurrencies, or wallets act as pass-through mechanism and are linked to cards or bank accounts.

[204] Worldpay-FIS, 2022 Global payments Report.

Figure 8: Share of payment instruments used at the POS in terms of value of transactions, 2016-2022, euro area



Source: ECB 2022 SPACE

More efficient payment infrastructures permitting credit transfers to take place within seconds have been developed, notably the Eurosystem's TARGET Instant Payment Settlement (TIPS) and EBA CLEARING's pan-European instant payment system, RT1. According to data from the European Payments Council for Q3 2022, instant payments (IPs) represented 13% of total volume of euro credit transfers in the EU.[205]

COVID-19 accelerated the rise of e-commerce, with 22% of EU enterprises reporting e-commerce sales in 2020[206], of which 19% reported that their online sales made at least 1% of their total turnover, one p.p. increase compared with 2019. In 2021, card payments were the most preferred payment method in e-commerce: credit cards accounted for 25% and debit cards for 17% of the total e-commerce transaction value in the EU[207]. Card payments were followed by digital payment wallets (including pass-through wallets; e.g. Apple Pay, Google Pay), which represented 27% of the transaction value in 2021.

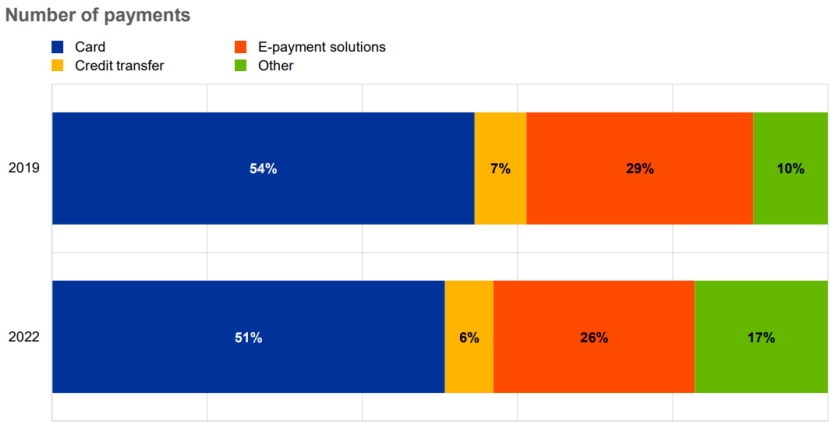
Offering more granular insights for the euro area, the 2022 ECB's SPACE report observes that online payments have become more frequent in comparison to POS and P2P across the euro area. In 2022, 17% of all day-to-day payments in 2022 were made online, compared with only 6% in 2019. In terms of value, the share of online payments was 28% (up from 14%) in 2022, suggesting that online payments were more frequently used for larger payment

---

205 European Payments Council, SCT Inst scheme – where are we now and where are we heading?
206 Eurostat, Online sales continue to grow among EU enterprises, December 2021.
207 Ibid.

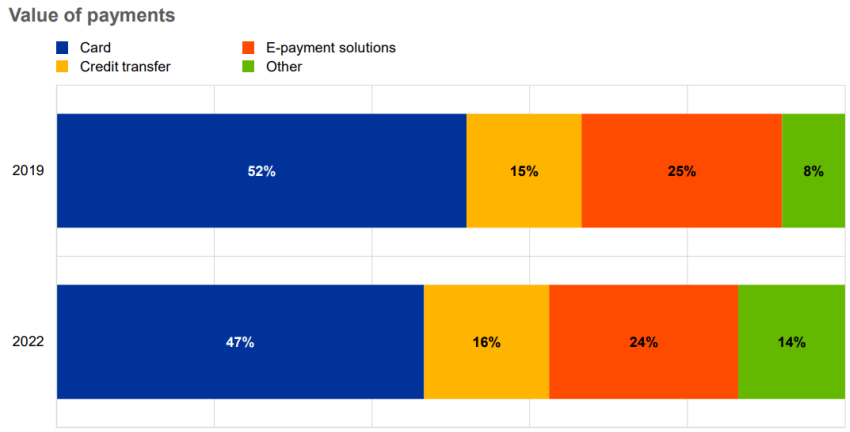
amounts. As noted in the report, at least 10% of all non-recurring transactions were online payments in every euro area country, a notable change, since online payments accounted for less than 5% of non-recurring payments in some countries (Malta, Cyprus and Germany) in 2019. In several countries the share of online payments in 2022 was over 20% (Belgium, Austria, Ireland and France). Whereas more than half of these online payments were still made with cards in 2022 (51%), this share has declined (even if only slightly, by 3p.p) between 2019 and 2022. The use of E-payment solutions including PayPal and other online or mobile payment method has also decreased slightly, whilst the share of a growing variety of other online payment methods (including direct debit, loyalty points, vouchers and gift cards, crypto assets, and any other methods) has risen to 17% (up from 10% in 2019) in terms of number of transactions and to 14% in terms of value (up from 8% in 2019).

Figure 9: Breakdown of number of online payments by payment instrument, 2019-2022, euro area



Source: ECB 2022 SPACE

Figure 10: Breakdown of value of online payments by payment instrument, 2019- 2022, euro area



Source: ECB 2022 SPACE

EU market for payment services

The PSD2 aimed at improving the provision of payment services across borders within the EU. With respect to this goal, a number of efforts have been made over the last years, such as the introduction of single euro payment area (SEPA) standards for euro transactions, the cross-border payment regulation[208], which equalised fees for cross-border and national payments in euros, and more recently with the current proposal on Instant Payments Regulation[209]. The ability for payment service providers to access the single market for payments through passporting rights has also contributed towards this goal. In particular, the number of third-party providers of payment services newly regulated under PSD2 which offer their services across borders beyond their home registration country has increased. According to Konsentus[210], out of the 353 fintech TPPs regulated in the EEA in Q4 2022, half of them passport their services into countries other than their home regulated market, which represents a 30% increase in relation to 2021[211]. More generally, the rise of online e-

[208] Regulation (EU) 2021/1230EC No 924/2009.

[209] Proposal for a Regulation Of The European Parliament And Of The Council amending Regulations (EU) No 260/2012 and (EU) 2021/1230 as regards instant credit transfers in euro, COM(2022) 546 final, 26.10.2022.

[210] About Konsentus | Helping Open Banking Stay Open & Secure. Konsentus provides insights into how Open Banking is developing in the EU and the UK, including a quarterly TPP tracker and country reports. In their research Konsentus only included the pure-TPPs, i.e. providers of only AIS and/or PIS, so not including banks (ASPSPs) that could also acts as TPPs.

[211] Konsentus TPP Tracker, Q4 2022.

commerce platforms has led to increasing demand for cheap and secure solutions for low-value transactions across borders[212].

Notwithstanding, the European payments landscape remains fragmented along national lines, with the uptake of innovative, digital solutions happening, to an important extent, in connection with. With regard to card payments, as noted by the ECB[213], a number of factors have contributed to the continued fragmentation of the market along national lines. First, while European cardholders are generally able to use their national cards at any terminal in Europe, the acceptance of cards issued under national card schemes across Europe has generally relied on co-badging with a very limited number of International Card Schemes (ICS). In the absence of a pan-European scheme for cards, co-badging has enabled PSPs to offer a user-friendly solution to the demand for a single payment instrument for national and cross-border payments[214]. Moreover, with the aim of facilitating cross-border acceptance, new banks often opt to issue cards with only ICS, including in countries where a national card scheme is available[215]. Finally, the introduction of interchange fee caps in 2015 has reduced national card schemes' price advantage on the acquiring side vis-à-vis international schemes.

With regard to credit transfers, the uptake of innovative payment solutions entailed with credit transfers (notably, PIS) and has been closely linked with the growth of domestic account-to-account (A2A) schemes. A2A schemes designate payments built on credit transfer rails offering consumers and merchants an alternative to cards. These have been importantly driven by domestic efforts, with many such schemes owned by ASPSPs or ASPSPs coalitions (although not all, e.g. Trustly, Klarna). For instance, schemes such as Giropay (Germany), iDeal (Netherlands), Swish (Sweden) and Bizum (Spain), facilitate A2A payments across the major banks in the respective countries. These schemes have grown considerably in terms of transaction volumes over the last few years, with Netherlands- based iDeal (from EUR 33bn in 2017 to EUR 99bn in 2021), Spanish Bizum (from EUR 1bn in 2018 to EUR 26bn in 2021) or Poland- based Blik (from EUR 1bn in 2017 to EUR 23bn in 2021) as illustrative examples[216]. In terms of market shares, these schemes still do not represent a large proportion of POS transactions (with Polish Blik presenting the most significant share, 15%, amongst a sample of recently surveyed markets[217]). This changes in terms of C2B e-commerce, with the cases of the Netherlands (75%), Poland (53%) and Belgium (47%) as the most prominent. The significance of these schemes is expectable to grow, with recent industry- led research[218]

---

212 Swift. (2018). The transformation of the European payments landscape. *Swift White Paper*, cited in the VVA/CEPS study, p.32.

213 ECB, "Card payments in Europe – current landscape and future prospects: a Eurosystem perspective", April 2019.

214 Ibid.

215 Ibid.

216 Van Arsdale, J., Majumdar, A., and Van Hoorn, M., European A2A Schemes Thriving, Not Yet Open Banking Payments, Flagship Advisory Partners, 28 October 2022.

217 Ibid.

218 Token.io, Who will pay by bank: Token and Open Banking Expo Survey Report, June 2022.

finding that 81% of EU consumers report they are "likely" to make an A2A payment in future.

However, while they build on the SEPA SCT and SCT Inst schemes, domestic A2A schemes pose issues of interoperability at the front-end across countries. In this context, the choice of payment options for cross-border transactions in the EU has remained limited for PSUs, with the majority of electronic PoI payments carried out or facilitated by a very limited number of ICS and BigTechs providing mobile payment applications based on ICS (e.g. Apple Pay, Google Pay, PayPal)[219].

Open Banking

As detailed in Annex 11, Open Banking under PSD2 covers account information services (AIS) and payment initiation services (PIS). AIS provide users with consolidated and/or analytical information on the basis of their payment accounts, while PIS offer account-to-account, non-card-based electronic payment solutions, notably in e-commerce. The regulatory framework of PSD2 has also allowed the emergence of 'API-aggregators'. In a context where the technical specifications of the data access interface available to TPPs have been left to ASPSPs, 'API aggregators' provide a single integrated API connection allowing Open Banking services providers to integrate with the different APIs provided by ASPSPs. In addition to API aggregation, some of these API aggregators also act as TPPs by offering their PSD2 license as a service to unlicensed fourth party Open Banking services providers.

When characterizing the current situation regarding the use of Open Banking in the EU, one difficulty concerns the lack of data on the use of TPP services. This is partly because institutions prefer to keep some user-data confidential, but also because there is no centralized regulatory database on the use of TPP services. Notwithstanding, data made available by industry research give an indication of how the EU landscape of Open Banking is evolving in terms of number of TPPs, users of Open Banking services[220] and API calls[221]. Moreover, the comparatively higher availability of data for the UK (through its Open Banking Implementation Entity) allows for reflections on how Open Banking in the EU compares with this non-EU market (cf. Annex 11).

According to Konsentus[222], the total number of TPPs in the EEA almost tripled in the period from September 2019 to Q4 2022, from 124 to 353 (of which 10 in non-EU countries)[223].

---

[219] Commission Staff Working Document Impact Assessment Report Accompanying The Document Proposal For A Regulation Of The European Parliament And Of The Council amending Regulations (EU) No 260/2012 and (EU) No 2021/1230 as regards instant credit transfers in euro; SWD(2022)546, p.12.

[220] 'Users' refers here to natural or legal persons using Open Banking services.

[221] An API call, or API request, is a message sent to a server requesting an API to provide a service or information. In the context of PSD2, an API call refers to the request sent by a TPP to the API of the ASPSP requesting access to account data.

[222] Konsentus is "*an infrastructure platform enabling safe and secure data exchange within open banking and open finance ecosystems*" - About Konsentus | Helping Open Banking Stay Open & Secure. Konsentus

TPPs in the EEA mostly provide either AIS (130), or a combination of AIS and PIS (202)[224]. This growth in the number of TPPs is not evenly distributed across the EU. In this regard, Konsentus data show that Sweden, Germany and Poland are the EU countries with more home registered TPPs (with 38, 36 and 30, respectively), while Spain, Italy and Germany have the highest number of passported TPPs (129, 128, 127).

With regard to the number of users of Open Banking services[225], there were 18.8 million users in Europe in 2021, up from 12.2 million in 2020, and forecast to grow up to nearly 64 million users by the end of 2024 (Figure 11)[226]. With regard to the number of API calls, research published in December 2021 by Konsentus estimated there were 570 million monthly API calls in Europe as of December 2019[227]. They expressed the expectation this would exceed 2 bn by December 2021, an increase of 350%, naming demand for Buy-Now-Pay-Later and Variable Recurring Payments as examples driving this increase. In an industry position paper by MoneyLIVE and Aiia (September 2022[228]), various Open Banking services providers refer to an increase in their API calls as of late. Aiia states that "*Open Banking payments have reached a tipping point*" in Europe, where it is no longer mostly the Nordics and the UK, but other countries are following.

---

provides insights into how Open Banking is developing in the EU and the UK, including a quarterly TPP tracker and country reports. In their research Konsentus only included the pure-TPPs, i.e. providers of only AIS and/or PIS, so not including banks (ASPSPs) that could also acts as TPPs.

223 Konsentus, Q4 2022 Konsentus Third Party Provider Open Banking Tracker.

224 Ibid.; data made available by Konsentus on type of TPP activity is not given per country and therefore does not allow to infer for EU countries only.

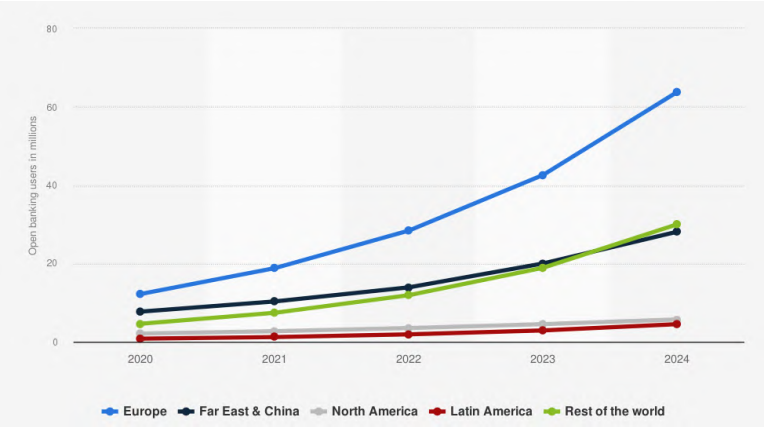
225 'Users' refers here to natural or legal persons using Open Banking services.

226 Statista, citing Juniper Research March 2021; available here.

227 Konsentus, Open Banking in Review: Trends and Progress, December 2021.

228 MoneyLIVE & Aiia, The Future of Open Banking Payments, 30 September 2022.

Figure 11: Number of Open Banking users worldwide in 2020 with forecasts from 2021 to 2024, by region (in millions)



Source: Statista, *citing Juniper research*

SCA/Fraud

SCA is now fully rolled-out and enforced throughout the EU. Latest figures on fraud related to card payments show a decrease in fraud in the EU. According to EBA data[229], the volume of fraudulent transactions from December 2020 to April 2021 fell by approximately 50% for issuers and by 40% for acquirers. In terms of value, the decrease was around 30%.

In spite of the reduction of the volume of fraudulent transactions, new types of payment fraud have emerged[230]. Fraudsters increasingly use 'social engineering' scams (e.g. phishing) in combination with sophisticated online attacks. SCA is not fully suited to prevent this type of fraud, as these transactions are generally authorised and authenticated through SCA.

Authorised Push Payments (APP) fraud is becoming more frequent. In the UK[231] around 189,000 APP scam cases on personal accounts were reported in 2021 (an increase of 30% on 2020) with a total value of GBP 506 million (a 46% increase on 2020). In Ireland[232] APP

---

229 European Banking Authority, Report On The Data Provided By Payment Service Providers On Their Readiness To Apply Strong Customer Authentication For E- Commerce Card- Based Payment Transactions, EBA/REP/2021/16, 2021

230 European Payments Council, 2022 Payment Threats and Fraud Trends Report, EPC183-22, 23 November 2022

231 UK Finance, Annual fraud report – The definitive overview of payment industry fraud in 2021 (August 2022).

232 FraudSMART, Payment Fraud Report (H2 2021), FraudSMART).

fraud rose by 15.9% in volume terms year on year in H2 2021 with an average APP fraud transaction amounting to EUR 4,237 in 2021. In Belgium the Service Public Fédéral Finances received, in 2022, 14.905 phishing reports, about 40 a day.[233] Also in Belgium, Febelfin reported, for 2020, 67.000 cases of phishing.[234] According to Banque de France, APP fraud corresponds to 59% of total fraud in value terms.[235] According to the EBA, credit transfers, due to the much higher average value of fraudulent transactions (EUR 4,190), show the highest aggregate value of fraud (EUR 310 million) in H2 2020, despite the lowest fraud rate overall; this generally translates to a significant impact on each affected customer, compared to other payment instruments.

SCA/Financial inclusion

Since the application of PSD2, the Commission has been made aware by market participants, including consumers,[236] that some authentication approaches, in particular those that rely on the use of smartphones, have led to exclusion of certain groups of society from using remote electronic payment transactions and online access to payment accounts.

4. EVALUATION FINDINGS (ANALYTICAL PART)

The evaluation of the PSD2 is structured around five assessment criteria defined by the Better Regulation Guidelines (effectiveness, efficiency, coherence, EU added value and relevance).

4.1 To what extent was the intervention successful and why?

4.1.1 Effectiveness

Summary assessment: Overall, the PSD2 framework has enabled progress towards its goals on competition, innovation, transparency and customer protection. Notwithstanding, some issues related to implementation, and regulatory and technical divergence have meant that the overarching goals of the PSD2 have not been fully met. Competition objectives are still hampered by an uneven playing field between ASPSPs and non-bank PSPs in terms of access to payment systems. In spite of the emergence of hundreds of new TPPs, there is still a fragmented landscape of APIs of varying levels of technical performance and functionalities, affecting the objective of broadening market access for TPPs. ASPSPs consider that this situation is the consequence of the prohibition of charging for the use of APIs. TPPs face costs and challenges related to connecting to thousands of bank APIs, not all offering to TPPs and their customers a seamless and frictionless journey. Significant progress towards customer protection objectives has been achieved by PSD2 provisions on SCA and liability

233 SPF Finances (belgium.be), Une année record pour le phishing.

234 Febelfin, Brochure_phishing_final_fr.pdf (febelfin.be)There is plenty of 'phish' in the sea - Fraude et escroquerie dans le secteur bancaire.

235 Observatory for the security of payment means, Annual Report 2021).

236 See notably BEUC, BEUX-X-2022-118_BEUC_position_paper_on_PSD2_review.pdf, page 12.

rules for unauthorized payments. However, new types of fraud (including Authorized Push Payment fraud) are developing and may not be remedied by current rules like SCA. As regards the objective to facilitate a Single Market for payments, despite progress in terms of an increase in the number of TPPs passporting their services beyond their home country, persistent inconsistencies in supervisory and enforcement mean that the EU market remains largely fragmented along national lines.

The effectiveness analysis considers how successful the PSD2 has been in achieving or progressing towards the five general objectives laid out in the 2013 PSD2 impact assessment[237]:

1) to ensure a level playing field between incumbent and new providers of card, internet and mobile payments;
2) to increase the efficiency, transparency and choice of payment instruments for payment service users (consumers and merchants);
3) to facilitate the provision of card, internet and mobile payment services across borders within the EU by ensuring a Single Market for payments;
4) to create an environment which helps innovative payment services to reach a broader market;
5) to ensure a high-level protection for payment services users (PSUs) across all Member States of the EU.

The success and limitations of the PSD2 framework in relation to its objectives (including those introduced in the summary above) are examined in greater detail below. Where relevant, this will be evaluated by considering how successful the framework has been in achieving the accompanying specific objectives laid out in order to facilitate the achievement of the general ones. In this respect, where the framework is considered to have been effective with regard to these specific objectives, it can be reasonably expected to also contribute to the general objectives. This section will consider, in relation to each objective, quantitative and qualitative effects of the intervention, external factors affecting progress towards the objectives, and unexpected or unintended effects driving or hampering progress ('Better Regulation Toolbox' Tool #47).

1) How successful has the PSD2 been in ensuring a level playing field between incumbent and new providers of card, internet and mobile payments?

Overall, PSD2 has allowed for greater competition as new businesses and business models have entered the market (as evidenced by the aforementioned increase in number of TPPs).

[237] Commission Staff Working Document SWD(2013) 288 final Impact Assessment Accompanying the document Proposal for a directive of the European parliament and of the Council on payment services in the internal market, 24.7.2013.

Notably, progress towards general objective 1 has been linked to the success of the PSD2 in meeting *the specific objective* of '*ensuring that emerging payment service providers are covered by the regulatory framework governing retail payments in the EU*'[238]. In widening the scope of the previous PSD, the PSD2 has been effective in covering two types of previously unregulated services - i.e. payment initiation services (initiating an online payment order) (PIS), and account information services (online services to provide consolidated information on one or more current accounts) (AIS).

The positive effect on competition has been reflected in stakeholders' sentiment. National supervisors consulted in the VVA/CEPS study have reported that, in regulating previously unregulated actors and services, as well as the security requirements for the interaction of ASPSPs with TPPs, the PSD2 created a clearer market structure and predictability (p. 92), progressing towards achieving competition-enhancing objectives. This was also echoed in the targeted consultation, with participants mostly agreeing that there is a wider choice of PSPs than before (86%, 106/123), and that the EU payment market is more competitive than before (77%, 96/125).

However, this perception changes with regard to how the level playing field between the different types of PSPs has evolved under PSD2, as reflected in stakeholder responses[239] to the targeted consultation, as well as in the Advice issued by the EBA (p. 3). Here, key issues limiting progress towards the goal of an even playing field relate to how the interaction between ASPSPs and TPPs is structured in the PSD2 framework, and to provisions on enforcement.

First, regarding the PSD2 requirement that ASPSPs provide TPPs with access to their customers' accounts free of charge, the costs of developing access interfaces to payment accounts have been seen to be a regulatory-driven 'competitive disadvantage' both by ASPSPs and TPPs. On the one hand, for several ASPSPs consulted in the targeted consultation as well in the VVA/CEPS study, the obligation to provide access to account data for free to TPPs has been perceived as imposing a one-side opportunity cost associated with developing access interfaces, where commercial benefits created for potential competitors have not been balanced by economic incentives for ASPSPs[240].

On the other hand, TPPs have noted that, as the regulatory technical standards (RTS) of PSD2 leave API standards to be set by the industry, API fragmentation across different ASPSPs, as well as across Member States, has put them in the disadvantageous position of bearing the costs of developing separate solutions to access APIs of different banks. In this respect, one unanticipated market development has been the appearance of new business models offering solutions to TPPs to facilitate their connection with end users' ASPSPs. Such

---

238 Specific objective 4 in the 2013 PSD Impact Assessment.

239 In this regard, it is worth noting that 30% of stakeholders participating in the targeted consultation have disagreed that the PSD2 has contributed to a levelling of the playing field.

240 See Annex 11, for further insight.

business models include API aggregation and 'license-as-a-service'. Research by Open Banking Exchange (OBE)[241] has shown that, by August 2022, 14 out of the 346 licensed TPPs in the EEA provided their license to fourth party providers, with the higher concentration of such companies found in France and Germany.

TPPs have also reported significant constraints with accessing accounts via some ASPSPs' APIs. Responses to the targeted consultation, as well as the EBA Advice, have identified a set of obstacles linked to the application of requirements on access to payment accounts, with an impact on the level playing field. These include obstacles to TPPs arising from the use of 'redirection' as a sole method of PSU authentication supported by ASPSPs, or additional friction in a TPP journey compared to that experienced by the PSU in the ASPSP interface (e.g. additional registration, consent and authentication steps).

With regard to the issues identified in relation to the access by TPPs to customer account data held by ASPSPs, and how these affect the goal of levelling the playing field between ASPSPs and TPPs, one dimension frequently noted in the targeted consultation (particularly by TPPs) as well as in the EBA Advice has been enforcement. While this will be further developed below (*cf. Obj.4*), it should nonetheless be noted here that progress towards competition goals have also been stifled by the limited effectiveness of provisions on enforcement.

The level playing field between ASPSPs and TPPs has also been affected by a divergent application of the provision allowing for an exemption from the requirement laid down in Article 97 of PSD2 to apply SCA where a payment service user is accessing the balance and the recent transactions of a payment account, provided that SCA was applied when the account information was accessed for the first time, and at least every 90 days after that.[242] The use of that exemption has led to divergent practices, with some account servicing payment service providers requesting SCA every 90 days, others requesting it at shorter time intervals, and some not applying the exemption, and requesting SCA for every account access. Users are often not aware that they need to renew their consent every 90 days, or not paying attention to the fact that their consent needs to be renewed to enable TPP accessing their data, and many TPPs therefore lost important revenue due to service interruption. This lead to friction in the customer journey when using account information services, and thus to a negative impact on account information service providers[243] which all mention this provision as being an important source of concern. Recently introduced provisions[244] amending the regulatory technical standards laid down in Delegated Regulation (EU) 2018/389 are expected to bring some relief by making this exemption mandatory and

---

241 Open Banking Exchange (OBE), *PSD2 TPP-as-a-Service*, Market Report (September 2022).

242 Article 10 of Commission Delegated Regulation (EU) 2018/389.

243 European Banking Authority, Draft Regulatory Technical Standards amending Commission Delegated Regulation (EU) 2018/389 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, EBA/RTS/2022/03, 5 April 2022.

244 Commission Delegated Regulation (EU) 2022/2360.

extending the period in between two SCAs to 180 days instead of 90. But even modified, this provision is still not fully satisfactory and more far-reaching solutions need to be considered in the PSD2 revision itself.

Finally, progress towards a level playing field has also been hampered by limited effectiveness of PSD2 provisions (Article 36) concerning non-bank PSPs' (more specifically Payment Institutions and E-Money Institutions) access to accounts maintained with a credit institution. Whereas PSD2 states that this should be provided on an objective, non-discriminatory and proportionate basis, to allow payment institutions to provide payment services in an unhindered and efficient manner, evidence gathered suggests that credit institutions are still often 'de-risking' PIs and EMIs by either refusing them access to a bank account or abusively closing bank accounts, thus fending-off competition by non-banks, unable to have or keep a bank account indispensable for carrying out their business or even for obtaining a license, as a bank account is indispensable to satisfy the safeguarding requirement of Article 10 PSD2, which is one of the authorization conditions. More precisely, responses to the targeted consultation have revealed a wide dissatisfaction among non-banks that there is no need for banks to notify or explain withdrawal of account access (only refusal of request for account access). In line with this, a clear majority (38 against 26 respondents, with non-banks and public authorities in the former group and banks in the latter) consider that Article 36 PSD2 should be modified, for example, by extending it to the termination of business relationships banks/non-banks. Furthermore, the EBA identifies in its Advice[245] divergent practices in relation to access to designated payment systems by PIs and EMIs, with some MS allowing for direct participation of PIs and EMIs in payment systems, whereas others do not, further impacting the level playing field.

2) **How successful has the PSD2 been in increasing the efficiency, transparency and choice of payment instruments for payment service users (consumers and merchants)?**

Overall, the PSD2 framework has had *a positive effect in increasing the choice of payment instruments for PSUs*.

Responses from the targeted consultation illustrate stakeholders' general perception that there are more options available to make payment transactions than five years ago (78%), and that PDS2 has contributed to market players developing more convenient payment solutions (60%). A similar sentiment was reflected in the outcome of the public consultation where the largest group of respondents were consumers, with 70% (66 replies) agreeing that the choice in payment services has increased over the last 5 years. A 2022 qualitative study by Kantar[246] commissioned by the ECB even concluded that, amongst both the general public and tech-savvy groups that were consulted, participants felt they were already well-served by existing

---

245 EBA Advice, p.100.

246 Kantar, Study on New Digital Payment Methods, March 2022.

payment methods, and rather than looking for something new, many were actively trying to reduce their payment options. Particularly, participants in the tech-savvy group reported that to consider a new payment method this would have to be an innovative product which would optimize and simplify (particularly acceptance across Europe), rather than increase their options[247]. Merchants taking part in the same study reported a trend towards accepting an increasingly wide range of payment instruments, primarily driven by customer preferences.

With regard to the Directive's success in ensuring that *payment services and instruments meet the needs of PSUs efficiently*, scarcity of data on the amount and number of PIS payments to merchants in the EU render difficult to assess whether the cost savings that the 2013 PSD2 Impact Assessment estimated for merchants from using PISPs and account-to-account-payments, instead of the more costly card payments, have been realized[248]. Notwithstanding, respondents to the public consultation reported that making digital payments has become easier (79%, 53 replies). This view was also held as regards making cross-border digital payments to other EU countries (69% find it has become easier), while only a minority (28%) agreed this has become the case for non-EU countries. Public consultation responses also suggest that this perception of an easy experience of non-cash payments is not hindered by SCA. Indeed, for physical, in-store payments, 44% indicate they find it easy (28 replies), against 30% (19 replies) who find it cumbersome. Moreover, of those respondents who reported finding the payment authentication experience cumbersome, around 20% (23% for physical, in-store payments, 22% for SCA during online payments) found SCA worth it as a fraud preventive measure (whereas an additional 20% reported 'other views' and neither found it worth it or not worth it). In contrast, industry stakeholders notably representing merchants' views consider that the SCA solution increases friction in the payment chain and customer journeys, potentially leading to customers not completing e-commerce transactions. Furthermore, legal uncertainties for corporates have been noted in relation with the transposition of Article 3(n) of PSD2, which excludes from the scope of the Directive payment transactions and related services between a parent undertaking and its subsidiary, or between subsidiaries of the same parent undertaking, if these are done without a PSP intermediary other than an undertaking belonging to the same group.

Regarding transparency, success has been more limited. Overall, responses to the targeted consultation under this topic indicate that most stakeholders somewhat agree that the transparency and information requirements of PSD2 are adequate (53%, i.e. 52 out of 98 responses), have contributed to making electronic payments more secure (56%), and have improved PSUs' understanding of their rights when using payment services (47%). Views were more divided on whether they have contributed to an informed user choice between different payment products, with those disagreeing in equal number to respondents who agreed (37% compared with 41%, with 22% neutral).

---

247 Ibid. pp.31 and 39.

248 However, as detailed in Annex 11, analysis of this data available for the UK suggests that this has not been the case.

Perceptions on effectiveness of transparency provisions also vary among stakeholders. Banking industry stakeholders consulted in the VVA/CEPS study as well as in the targeted consultation expressed discontent with requirements regarding provisions on information (contract conditions, information about executed payments). In particular, the two-month period for notifying changes to framework contracts[249] is considered ineffective where the change is beneficial for the consumer.

Several ASPSPs also expressed the view that consumers still lack an adequate understanding of data to which they are granting access, as well as of how this data is used (and potentially monetised). Relatedly, ASPSPs consulted in the VVA/CEPS study regretted that with business models such as API aggregators (where, as introduced previously, the provider of an integrated API solution facilitates the connection between an Open Banking service provider and several distinct ASPSPs' APIs) the ASPSP has no overview of the fourth party provider which is accessing the customer data via the aggregator.

From the TPPs side, one European TPP industry organization expressed, in the targeted consultation, the view that Article 45(2) of PSD2 requiring their business information to be provided to the PSU prior to initiation means that PISPs cannot effectively compete with card payments, where neither the card acquirers nor the card processors have such obligations.

PSUs' views expressed in the targeted consultation also point to limitations to the success of PSD2 provisions on transparency. On the merchants' side, views expressed were that, under Article 45(2) (a) and (b), card-based and non-card-based payments do not share the same regulatory burden in terms of information and transparency requirements. On the consumers' side, the view expressed is that information provided by PISPs before the execution of a transaction is not clear enough, as it is very difficult for a consumer to find the document indicating where the PISP is registered, and the contact details of the competent authority. In line with this, the ERPB in its 2022 report[250] found that often the merchant's commercial name provided did not allow the payer to identify to whom a payment transaction had been sent, because the name, while legally valid, was not a name by which the payer was able to easily identify the merchant. The ERPB also identified that there are several cases where providing accurate information on the location of a purchase is difficult, misleading or of limited value, e.g. itinerant traders (namely, taxis and other related services), and services offered and paid for at the home of the consumers.

Finally, PSD2 has also sought to deliver progress on this objective by enhancing transparency of cross-border transactions within the EU and with other jurisdictions. However, one difficulty stifling progress on this goal concerns disclosure of currency conversion charges applied by PSPs to one-leg out credit transfers/remittances. In this regard, views expressed in the targeted consultation on whether currency conversion costs should be disclosed before

---

249 Article 52(1).

250 Final report of the ERPB working group on transparency for retail payments end-users (europa.eu).

and after a payment transaction[251] were divided. While PSPs disagreed, TPPs, consumers and merchants were favorable to such a change[252]. Besides impacting progress on the PSD2 transparency objectives, lack of price transparency is also a leading factor heightening remittances costs, according to the World Bank[253], limiting the ability of the EU to deliver on its commitment to achieving the G20 and SDG targets on remittances costs reduction to 3% by 2030. Furthermore, the VVA/CEPS study also reports that consumer awareness about new types of PSPs, whether they are supervised or trustworthy, remains low[254]. This is especially the case with regard to cross-border transactions within the EU, with consumers often unaware of the classification of the service provided, the provider, the applicable legal framework, and the competent supervisors.

3) How successful has the PSD2 been in facilitating the provision of card, internet and mobile payment services across borders within the EU by ensuring a Single Market for payments?

The PSD1 framework already had some success in developing cross-border payment services within the EU and enhancing the quality of such services[255]. Still, the PSD2 has enabled some additional progress towards the goal of developing an EU single market for payment services. Notably, according to an EBA survey in March 2019[256], 45% of authorized PSPs were using or planning to use the EU passporting regime to provide cross-border services. Konsentus data for the EEA indicates that the number of TPPs passporting into another country has increased from 39 in Q3 2019 to 175 in Q4 2022[257].

This increase in the number of PSPs offering payment services across borders in the EU evidences some success of the more streamlined framework for passporting notifications under PSD2 as compared to PSD1[258]. The Directive also added clarity with regard to the information to be provided when a payment institution or e-money institution is using an agent and when an e-money institution is using a distributor. These regulatory changes have

---

251 Similar to the current rules for two-leg payment transactions that involve a currency conversion included in the Cross-Border Payments Regulation.

252 In addition to evidence from the targeted consultation, a 2022 Remittances Report by Wise concluded that banks in EU are still largely failing to comply with requirements to disclose 'all currency conversion charges' up front for European transfers, identifying ineffective enforcement as key issue.

253 World Bank, Ending remittance hidden fees: the international community calls for action.

254 VVA/CEPS study, p. 97; also EBA/REP/2021/04.

255 Commission Staff Working Document (SWD/2013/0288 final) Impact Assessment Accompanying the document Proposal for a directive of the European parliament and of the Council on payment services in the internal market, 24.7.2013.

256 EBA Report on The Impact Of Fintech On Payment Institutions' And E-Money Institutions' Business Models, July 2019.

257 Konsentus, Q4 2022 Third Party Provider Open Banking Tracker.

258 The passporting regime allows Payment Institutions authorised in one Member State to carry out activities in any other EEA state without additional authorisation. The PSD2 was accompanied by new Regulatory Technical Standards on the framework for cooperation and exchange of information between competent authorities for passport notifications.

contributed towards the specific objective of better aligning licensing rules for payment services across Member States. Nonetheless, some issues have remained which have limited progress towards general objective 3 and specific objective 5, 'to improve the consistent application of the legislative framework across Member States' and 'to better align licensing and supervisory rules for payment services across Member States'.

Notably, one limitation to the success of the PSD2 framework on the above-mentioned passport notifications for agents and distributors has been a divergence in practices amongst NCAs in assessing whether cross-border activities carried out by PIs and EMIs using agents or distributors fall under the ROE or the FPS. As noted in the EBA Advice to the Commission on the review of PSD2[259], such divergences stem from the absence of clear criteria in the EU legislation to delineate between the ROE and FPS, potentially leading to disagreements between NCAs and/or between NCAs and PSPs as to the applicable regulatory requirements and supervisory powers. This also impacts the effectiveness of the PSD2 with regard to transparency goals, due to difficulties ensuing for consumers in identifying the applicable consumer protection measures, as well as the relevant authority for specific supervisory purposes and complaints handling.

In addition, the EBA has also identified divergent approaches amongst NCAs to how passporting notifications should be treated in the case of the so-called "triangular passporting"[260]. In particular, NCAs have taken divergent interpretations regarding the permissibility of such passporting notifications that are not explicitly envisaged in the PSD2. Such form of "triangular passporting" creates uncertainty in the provision of payment services across borders by making it difficult to determine which AML/CFT and consumer protection regulations are applicable to the services provided by the intermediary in the host Member State. It also poses supervisory challenges in terms of the supervision of the activities carried out in the host Member State (including from an AML/CFT perspective).

A second limitation concerns the lack of consistency in how the definition of "payment account" is interpreted across the EU. In this regard, the EBA observed (p. 12) that there have been different interpretations leading, in particular, to questions as to whether certain types of accounts, such as electronic money accounts linked to prepaid cards, savings accounts, reference accounts, credit card accounts and others, should be considered payment accounts. This has led to uncertainty regarding the different types of account data which can be accessed by AISPs and PISPs across the EU, with, for instance, AISPs accessing credit card data in some jurisdictions but not in others. Thus, the lack of clarity in the definition of payment accounts remains a limitation on the effectiveness of the Directive with regard to its objective of facilitating the provision of payment services across borders, but also to its Open Banking goals (*cf. Obj. 4*).

---

[259] Page 50 and following.

[260] When a PI/EMI authorised in a country "A" uses an intermediary (such as an agent, distributor or branch) located in a country "B" for offering payment services in another country "C".

A third issue concerns the divergence across Member States in their approaches to the authorisation of payment services linked to a payment account, as well as to the services linked to 'the operations required for operating a payment account' as set out in items 1 and 2 of Annex I to PSD2. A case in point are the authorization requirements for PIs. Accordingly, with regard to opening and maintaining a payment account of the PSU, some jurisdictions have taken the approach to require PIs to be authorised for services under items 1, 2 and 3 of Annex I to PSD2, whereas in other jurisdictions PIs can open and maintain payment accounts of the PSU and provide individual payment services without such requirement. Also, with regard to the services of issuing of payment instruments and acquiring of payment transactions, the EBA identified divergent approaches in the authorisation of PIs, with some NCAs requiring PIs also to be authorised for the execution of payment transactions under items 3 or 4 of Annex I to PSD2.

A fourth issue limiting effectiveness of the Directive with regard to its goals of furthering the EU single market in payments concerns the lack of harmonisation in the application of the methods for the calculation of own funds of PIs across the EU under Article 9 of PSD2. More precisely, the EBA notes a divergence in the application of the requirement on who should be responsible for choosing the method for the calculation of own funds where, at times, PIs were allowed to choose the method, potentially leading to regulatory arbitrage.

Finally, both the VVA/CEPS study and the EBA reported concerns by PSPs regarding differences across national authorities in terms of the duration of the application process, as well as the regulatory requirements for operating across borders. Besides making such activities difficult, one effect is the scope for regulatory arbitrage, as firms can passport their service across the EU after having established themselves in one Member State (for which there might be more or less regulatory requirements to do so).

4) **How successful has the PSD2 been in creating an environment which helps innovative payment services to reach a broader market?**

The PSD2 has laid important stepping-stones towards its goal of enabling innovative PSPs to reach broader markets by outlining the regulatory foundations for an Open Banking framework in the EU, particularly the framework for access to customers' account data held by ASPSPs. As further detailed in Annex 11, the PSD2 has enabled TPPs (PISPs and AISPs) who build on ASPSPs' existing data and infrastructure to provide PSUs a range of new services for managing their finances, and/or providing cheaper payment solutions.

As noted previously, PSD2 provisions on account data access have been successful in augmenting the EU market in Open Banking services in terms of number of new TPPs, number of users of Open Banking services, and number of API calls. While numbers of Open Banking services users and API calls suggest that the Directive has been successful in broadening market access for PSPs, experience acquired during the implementation of PSD2 has also revealed important limitations on progress towards this objective. As already mentioned above the limitations relate to the lack of remuneration incentives reported by

ASPSPs for providing quality APIs, the limited quality of access by TPPs to account data, and difficulties related to supervision and enforcement.

First, ASPSPs consulted in the VVA/CEPS study and target consultation expressed the view that current provisions establishing that access to customers' account data shall be provided for free have stifled innovation by ASPSPs both in terms of developing high-quality access mechanisms and introducing new functionalities to customers. Accordingly, many ASPSPs noted in the targeted consultation the lack of a fair distribution of costs and opportunities between parties involved, where the (high) costs of developing access interfaces have not corresponded to the benefits and have mostly been borne by the banks. In addition, the EBA has noted that the PSD2 does not currently provide clarity on the delineation between access that must be available free of charge, and "premium" data services or added-value functionalities that go beyond the scope of the PSD2 requirements. Moreover, several banking industry stakeholders (including industry associations and ASPSPs) argued that the free access regime and lack of clarity concerning beyond PSD2 baseline, value-added data access services means that it is not commercially profitable for ASPSPs to introduce new functionalities, as implementing the functionality to the API makes the building costs double.

On the other hand, free access to customer account data held by ASPSPs has been appreciated in views expressed in the targeted consultation by associations representing consumers, as well as by several TPPs. Accordingly, although both sides expressed agreement with the possibility of ASPSPs and TPPs agreeing on a remuneration for services beyond the PSD2 baseline, they also noted that baseline account data should remain free to keep data ownership with customers and market entry barriers low.

One development likely related to the lack of commercial interest and economic incentives of ASPSPs for developing access interfaces, as the EBA (EBA, p. 87) has observed, has been an overreliance by some ASPSPs on the use of the customer interface as a primary or fallback access interface for TPPs. In particular, some small and medium sized ASPSPs offer only their adapted customer interface as a primary access method for TPPs and have chosen not to provide an API. In this respect, it is the EBA's view that the choice given to ASPSPs to use their customer interface as fallback access mechanism does not create incentives for ASPSPs to provide and use high-quality APIs, while it increases the efforts that TPPs must put into integrating different customer interfaces (EBA, p. 88). In contrast, the views expressed in the targeted consultation by some TPPs as well as a stakeholder representing TPPs (ETPPA) were that, given the different APIs set up by ASPSPs as well as, oftentimes, their insufficient quality, free access via ASPSPs direct user interfaces must always be an option to access account data.

Second, TPPs consulted in the VVA/CEPS study as well as the targeted consultation have reported several difficulties hampering access to PSUs' data. Such problems include missing or inconsistent data, but also a gap between PSD2 API and ASPSP's other customer-facing interfaces, with authentication methods, data exchanges and ease of use of the PSD2 APIs not matching the experience offered by the ASPSP's in their other customer-facing interfaces. Low quality APIs have also impaired TPP's authentication procedures (particularly where

redirection is used), negatively affecting their user experience of authentication flows on mobile devices, while an increasing number of consumers use their mobile devices for AIS and PIS services.

This issue with the quality of the access to account data has been linked by some stakeholders responding to the targeted consultation to the lack of specific API standards in the regulatory technical standards (RTS) of PSD2 (PSD2's Open Banking provisions set a performance criterion for APIs, but standards are left to industry). Indeed, while views on whether current provisions lacked more precise standards were divided, a relative majority (53%) agreed that this was the case. Those in disagreement (mostly ASPSPs and ASPSP industry representatives[261]), highlighted the funds already invested in building an access interface, and the additional costs which would need to be committed with no guarantee that it would solve any issues as there is no program manager responsible for running Open Banking at a pan-European level. These stakeholders also noted that a standardization approach would go against the technology neutrality principle. While support for common standards was mostly found amongst public authorities and consumer organisations, TPPs who also agreed see the lack of API standardisation as resulting in a fragmented market where TPPs must develop tailored solutions to connect to the different APIs of each ASPSP. Moreover, even though domestic API standards have been established in some Member States, cross-border interoperability in terms of access to data remains low. One example is France, where harmonised API standards have been implemented by the country's six major banks[262] and through their jointly-owned processing company, STET, whereas foreign banks operating in France adopted their own API standards often based on the 'Berlin Group' standard[263]. On the other hand, various TPPs noted in the targeted consultation that what currently lacks are common minimum user experience requirements to ensure an acceptable level of quality concerning access to data, and that framework should thus be principles- rather than standards- based, to allow innovation.

Thirdly, limitations to market access faced by TPPs have been linked, as previously noted (*cf. Obj. 1*), to shortcomings identified in relation to supervision and enforcement. One key supervision-related issue affecting effectiveness of the Directive's Open Banking provisions concerns the lack of consistency in the definition of "payment account" across the EU. This has implications in terms of differential access by AISPs and PISPs to different types of account data, with AISPs for example accessing credit card data in some jurisdictions but not in others. In this respect, although the CJEU ruling C-191/17 and Q&A 4272 has brought some clarity to the market on how the term 'payment account' should be interpreted, the EBA has noted in its Advice that the ruling is based on the provisions in the PAD rather than the PSD2. It also notes that, if applied directly to PSD2, these provisions would significantly narrow down the scope of the payment accounts under PSD2. As a result, lack of clarity in

---

261 Including European Savings and Retail Banking Group and European Banking Federation.

262 BNP Paribas, Crédit Agricole, BPCE, Crédit Mutuel, Société Générale and HSBC.

263 The 'Berlin Group' is a pan-European payments interoperability standards and harmonisation initiative.

the definition of payment accounts remains a limitation on the effectiveness of the Directive with regard to the objective of enhancing market access for TPPs.

In terms of difficulties in accessing payment account data held by ASPSPs, TPPs have noted that, when discrepancies are pointed out to ASPSPs (non-compliance), the speed at which ASPSPs respond and solve the issue, or the adequacy of response, differs. Another common complaint reported in the targeted consultation has related to cases where ASPSPs have received an exemption from the obligations to set up a contingency mechanism under Article 33(6) of the RTS on SCA&CSC but are no longer complying with the conditions. Here TPPs have stressed the need for NCAs to initiate a process to revoke the ASPSP's granted exemption. Regarding these issues related to the implementation of data access interfaces, many TPPs have stressed the ineffective enforcement by regulators, with some also noting the lack of a program manager responsible for managing and enforcing Open Banking at a pan-European level (like the OBIE in the UK).

The problem of inconsistent and/or lagging enforcement of provisions on payment account data access has also been noted by the EBA in its Advice, which highlights a number of challenges reportedly faced by NCAs in relation to enforcement. These include the significant time, resources and specific skills needed to supervise technical specifications of innovative IT systems and solutions, or the high-level requirements in PSD2 and the RTS on SCA&CSC which have led to uncertainties in the interpretation of certain provisions (for example, on the functionalities that ASPSPs' dedicated interfaces must meet).

Finally, PSD2 provisions have not been fully effective as far as consent and permission management are concerned. More precisely, the specifics of consent associated with an ASPSP's PSD2 API sometimes mean that the PSUs may not be correctly informed of what their consent means[264]. This problem is worsened by prevailing challenges in terms of consumers' financial and data literacy. Particularly, the lack of understanding of Open Banking and concerns regarding privacy and data sharing may result in reluctance to engage with new digital methods, as well as enduring preference for banks as PSPs.

Accordingly, survey data by Mambu[265] in March 2021 suggested that "*customers still do not get the term 'Open Banking'*", and that "*when customers use Open Banking, they do it without realising what it is*". Notably, of the 2,000 banking customers sampled, 52% had never heard of 'Open Banking'. Moreover, although many customers confirmed using one or more finance-apps (80%), 61% said they never use Open Banking, largely due to data sharing concerns (57%). In the public consultation, responses received (66) with regard to the use of

---

[264] This is particularly the case with regard to Article 10 RTS. Moreover, it also flags the issue of coherence between definitions of consent in PSD2 and in GDPR, further developed below (cf. 4.1.3).

[265] Mambu: Disruption Diaries – Let's talk openly - What do people think about Open Banking today? And where are the opportunities for banks and others to create value? [Results of Mambu's global Open Banking consumer survey], April 2022. Mambu-Disruption-Diaries-Open-Banking-Report.pdf (openfuture.world).

Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs) have shown that 45% (30) of respondents use either one or both services, whereas the remaining either do not use the services (24 – 36%) or do not know/do not provide an answer (9 and 3, 14% resp. 5%). The most common reason provided for not using these services was not wanting to share data with other companies than their own bank (15 responses – 23%) and that they do not trust these providers (12, 14%) [266].

5) How successful has the PSD2 been in ensuring a high level of protection for payment services users (PSUs) across all Member States of the EU?

The PSD2 has enabled considerable progress with regard to its objectives on protection of PSUs interests (*general obj.5* and *specific obj.6*) by introducing changes to the security requirements, which have been effective in limiting fraud (see below), but also by reducing the payer's liability for unauthorized payments and ensuring unconditional refund rights for direct debits in euro.

The EBA's regulatory technical standards (RTS) specified changes in the strong customer authentication (SCA) and common and secure communication (CSC) obligations in access to account information electronic payment initiation and remote channel actions. These provisions have been effective in enhancing the protection of PSUs by decreasing the risk for customers of fraudulent transactions. In effect, EBA data[267] showed that, even for a reporting period (H2 2020) when many acquirers, issuers and merchants in the EU were still not compliant with SCA requirements, fraud rates were significantly lower for payment transactions where SCA was applied compared to those where SCA was not. More precisely, with regard to remote card payments, SCA authenticated transactions have a 70-80% lower share of fraud in the total volume and value of transactions than those without (cf. figure 5). This correlation between SCA and a lower fraud rate was also observed with regard to non-remote card payments.

[266] These findings echo those from other studies. In the qualitative study conducted by Kantar, Study on New Digital Payment Methods (March 2022), this concern with privacy and data sharing was found equally in the case of, as well as amongst the unbanked, underbanked and offline population. In relation to this concern, both the general public and the tech-savvy group expressed having a higher level of trust in banks, while the latter group also reported a distrust in banks.

[267] European Banking Authority, Discussion Paper On EBA's Preliminary Observations On Selected Payment Fraud Data Under PSD2, As Reported By The Industry, EBA/DP/2022/01, 17 January 2022.

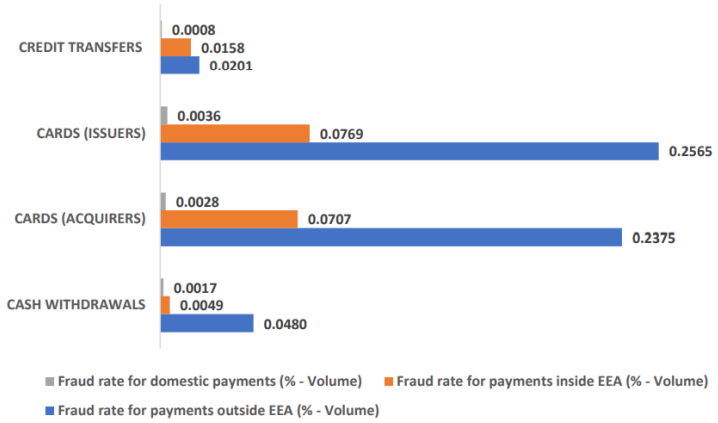
Figure 12: Fraud rate for remote card payments reported by issuers and acquirers, with and without SCA

Source: EBA/DP/2022/01

Moreover, the correlation is even stronger when looking into the cross-border card transactions, in particular those with counterparts located outside the EEA, and therefore outside of the scope of the SCA requirements under PSD2 and the EBA's RTS, further evidencing the effectiveness of these provisions. 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)[268].

[268] Ibid.

Figure 13: Fraud rate when payments are executed domestically, inside EEA and outside EEA



Source: EBA/DP/2022/01

The reductive impact of SCA on fraud rates does not, however, seem to materialize in the case of remote credit transfers. Here, while credit transfers are the payment instrument for which the fraud rate is the lowest (both in terms of volume and value)[269], the fraud rate is higher for SCA authenticated payments compared to payments that are not authenticated with SCA. As the EBA report notes, however, the EBA Guidelines on fraud reporting under PSD2[270] determine that non-SCA authenticated transactions are transactions for which an exemption to SCA under the RTS on SCA&CSC was applied, or for which SCA was not applied due to other reasons (e.g. merchant-initiated transactions or one-leg transactions for card-based transactions). One explanation for this higher fraud rate in the case of remote credit transfers might thus be that payments for which an exemption was applied (such as for example the low-value payment exemption in Article 16 of the RTS) constitute lower-risk transactions.

At the same time, it is important to read the high number of SCA-authenticated yet fraudulent transactions in light of recent transformations in fraud practices and techniques. Accordingly,

---

[269] More specifically, as the EBA reports, the fraud rate for H2 2020 ranges from 0.0012 % of the total volume of credit transfers compared with 0.0345 % of the total volume of card payments reported by acquirers (i.e. a rate that is 29 times higher than that for credit transfers). Also, the fraud rate in the same period ranges from 0.0011 % of the total value of credit transfers, compared to 0.0458 % of the total value of card payments reported by acquirers (i.e. a rate 42 times higher). EBA/DP/2022/01, p.11.

[270] European Banking Authority, Final Report on Fraud Reporting Guidelines under PSD2, EBA/GL/2018/05 (consolidated version), 18 July 2018.

as detailed in the European Payments Council's 2022 report on Payment Threats and Fraud Trends[271] the implementation of SCA provisions has been followed by a growth in new forms of fraud like phishing, spoofing and other social engineering techniques whereby fraudsters manipulate payers into making fully authenticated transactions (Authorised Push Payment fraud).

PSD2 provisions have enabled progress in protecting consumer interests (*specific objective 6*) in areas beyond fraud risk such as reduced liability for unauthorized payments and unconditional refund rights for direct debits in euro. The Directive has also enhanced consumer rights when sending transfers and money remittances outside the EU or paying in non-EU currencies by extending PSD1 rules on transparency to "one-leg transactions", hence covering payment transactions to payees outside the EU as regards the "EU part" of the transaction.

Merchants and PSPs have noted that, although the increased protection ensured by SCA requirements has the potential for reassuring customers regarding e-commerce, it has also meant more barriers in the customer journey to completing a transaction. Furthermore, the technologies and the processes required to ensure the correct implementation of SCA have been noted to be prescriptive, and biased towards mobile technologies users. Notably, the EBA (p. 83) notes that some authentication approaches, in particular those relying on the use of smartphones, have led to exclusion of certain groups of society from remote electronic payment transactions and online access to payment accounts as fundamental financial services. The potential exclusion of certain populations of less tech savvy customers, those that do not have access to digital channels/devices, customers with specific disabilities and elderly people constitutes an important limitation in the effectiveness of the provisions with regard to the goal of ensuring safe and high-quality payment services to all customers.

4.1.2 Efficiency

Summary assessment: According to the VVA/CEPS study, the largest cost items associated with the implementation of PSD2 are linked to Open Banking and in particular API-development, followed by SCA roll-out (implementation costs and increase in transaction failure rates) and legal interpretation/uncertainty. These costs are offset by benefits for TPPs, credit institutions and consumers, most of which come from the improvement of the functioning of the single market, followed by unlocked potential for innovation and a more secure payment environment. National authorities and TPPs established before PSD2 was introduced were more positive about the general impact. While a large part of the costs of the PSD2 were incurred in the initial stages (i.e. substantial investment costs), the benefits – although significant – only materialise gradually and it is therefore difficult to draw an overall conclusion regarding costs and benefits at this time, as only few years have passed

[271] European Payments Council, 2022 Payment Threats and Fraud Trends Report, EPC183-22, 23 November 2022.

since the PSD2 has been fully implemented. 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.

The efficiency analysis assesses the benefits and costs arising from the EU intervention and whether it was cost effective. The analysis also assesses opportunities for simplification and maximisation of benefits.

The efficiency analysis is based to a large degree on the cost-benefit analysis of the VVA/CEPS study. The results must be seen under the caveat that 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 in the VVA/CEPS study 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 were only assessed based on assumptions. In addition, 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.

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

- Open Banking and in particular API-development (estimated at EUR 2.2 billion)
- SCA rollout, notably implementation costs (estimated at EUR ~ 5 billion) and an increase in transaction failure rates (estimated in the VVA/CEPS study at up to EUR 33.5 billion). However, the value of failed transactions is not a cost. Only a small fraction of this is opportunity cost (e.g. unrealised profit /value added on those sales[272])
- Legal interpretation and uncertainty

Figure 14: Costs linked to PSD2

Cost item	Stakeholders included in calculation	Value (if relevant, year)	Type
Development of application programming interfaces (APIs)	Credit institutions	Total: EUR 2,200,000,000* Small and medium ASPSPs: 430,000€ Large ASPSPs: 14,800,000€ **According to the VVA/CEPS*	One-off

[272] It is also reasonable to assume that most of these sales takes place in alternative channels (e.g. brick- and mortar shops), or by alternative payment means. Therefore, at societal level the value of lost sales is much lower than the value of failed transactions.

Cost item	Stakeholders included in calculation	Value (if relevant, year)	Type
		study; however, these costs are very likely to be overestimated, as there is no segregation of costs and overall most would be linked to adapting their IT systems including for security/cloud computing.	
SCA implementation	Credit institutions, TPPs, merchants	Total: 5,000,000,000 € ASPSPs: small - 2,224,900,000 € ; large - 1,639,100,000 € TPPS : micro - 8,200,000€ ; small to large - 275,900,000 € Merchants: 836,000,000 €	One-off
Development of products based on APIs	TPPs	140,000,000-285,000,000 €	One-off
Business loss due to SCA implementation (friction and complexity of authentication method)	Merchants	[~33.500,000,000 €*] **According to the VVA/CEPS study; however, only a small fraction of this amount can be accounted for as an opportunity cost*	One-off
Registration costs for new TPPs	TPPs	10,000,000 €	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 (i.e. education campaigns)	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
Reduced revenue from acquiring and issuing scheme fees	Card schemes	Too early to call	Recurring
Less room to steer consumers to cheaper means of	Merchants	Too early to call	Recurring

Cost item	Stakeholders included in calculation	Value (if relevant, year)	Type
payment (surcharge ban)			

Source: VVA/CEPS study

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 EUR 1.6 billion)
- Unlocking the potential for innovation, especially when it comes to modernization of IT infrastructure, Open Banking, the further development of consumer services (like financial planning tools)
- More secure payment environment for customers and a reduction in fraud rates (worth EUR ~0.9 billion per year)

Figure 15: Benefits linked to PSD2

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[273]	~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: VVA/CEPS study

According to the VVA/CEPS study, a majority of credit institutions and banking associations consulted for the study suggested that the costs of the PSD2 largely outweigh the benefits. National authorities and TPPs established before PSD2 was introduced were more positive about the general impact, but they tended to agree with the overall assessment. This is also in line with the responses received to the targeted consultation. As regards the question whether the aggregated benefits stemming from the implementation of PSD2 outweigh its implementation costs, only 18 (27%) respondents answered with "yes" and 48 (73%) with "no". Of the 48 respondents who gave a negative answer, 29 (60%) are from the banking sector.

[273] Eventually, even if fraud costs are borne partly by card issuers, they pass on these costs to the end uses (consumer) in the form of higher prices (or provide less benefits from the interchange revenue).

Opportunities to simplify the level 1 legislation generally relate to the reduction of legal ambiguity, i.e. the large room left for interpretation by NCAs leading to inconsistent application, and to the improvement of the interplay with other legislation. In addition, stakeholders would be in favour of a more technology-neutral legislation, a comment generally made both for APIs and SCA, which in their view would reduce burden. Specific aspects related to level 2 legislation, namely the '90-day rule' (see above page 22) and technology neutrality were also considered as having simplification potential.

Stakeholder feedback was generally positive on the potential for simplification (in the case of the survey, 71% believed there is potential).

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 – although there is a lack of substantiated evidence as to their level) would also be difficult to lower.

4.1.3 Coherence

Summary assessment: Overall, the PSD2 shows a high degree of internal coherence. In terms of external coherence, the assessment shows that coherence with other EU legislation such as the E-Money Directive, the Digital Operational Resilience Act, the Crypto Asset Markets Regulation and the General Data Protection Regulation needs to be slightly improved.

In assessing how the PSD2 fits into a broader overarching architecture, the degree of coherence between the provisions of the Directive (internal coherence) as well as its relationship to other interventions (external coherence) has been analysed.

4.1.3.1 Internal coherence

Overall, the Directive shows a high degree of internal coherence[274]. Some minor inconsistencies were identified, for example, between the Chapter on framework contracts and single payment transactions. The obligation to inform the payment service user about ADR procedures is only intended for framework contracts, but also appears justified for single payment transactions. Similarly, the EBA noted that the Chapter on single transactions refers to PSPs and PISPs separately, while the Chapter on framework contracts only refers to PSPs[275].

[274] VVA/CEPS study, p. 184.
[275] EBA Advice (EBA/Op/2022/06), p. 58.

4.1.3.2 External coherence

Interchange Fee Regulation

The PSD2 is complemented by Regulation (EU) 2015/751 (IFR). To foster the Internal Market and competition in EU card payments, the IFR harmonizes diverging laws and administrative decisions and addresses restrictive business rules and practices. The IFR introduced caps for hitherto high interchange fees for consumer debit and credit cards, therefore setting harmonized ceilings for interchange fees for consumer cards in the EEA, and business rules aiming at removing barriers to the internal market, such as restrictions on cross-border acquiring or the prevention of choice of payment brand or payment application for consumers and merchants. The IFR is closely related to PSD2, as the card-specific provisions of PSD2[276] complement the IFR in promoting entry, including of pan-European card schemes or in preventing payees from requesting charges for the use of payment instruments for which the interchange fees are regulated in the IFR. No coherence issues have been identified with regard to the IFR.

E-Money Directive

Directive 2009/110/EC (EMD2) sets out the rules on the business and supervision of electronic money (e-money) institutions in order to contribute to the emergence of a true single market for e-money services in the EU. The EMD2 is applicable since 30 October 2009. In its Advice, the EBA has identified a number of divergences between the two legal frameworks[277]. Most prominent issues concern the difficulties in distinguishing between "*payment account*" and "*electronic money account*", between "*payment services*" and "*electronic money-related services*", as well as between "*scriptural money*" and "*electronic money*". The EBA also identified differences in some of the applicable legal requirements related to authorisation, own funds and safeguarding. The nature and status of distributors of electronic money[278], as well as the treatment of pre-paid instruments and whether they are based on electronic money in all cases were also identified as challenging to deal with. For these reasons, both the EBA and the VVA/CEPS study have advocated merging PSD2 with EMD2.

---

[276] For instance, article 62 governing charges levied by payees on payers in respect of card-based payment transactions or 65 PSD2 on the confirmation on the availability of funds upon the request of PSPs issuing card-based payment instruments.

[277] EBA Advice (EBA/Op/2022/06), p. 27 et seq.

[278] The EBA is of the opinion that distributors and their respective obligations have not been properly defined in EMD2, where Article 3(4) of EMD2 only prescribes that EMIs shall be allowed 'to distribute and redeem electronic money through natural or legal persons which act on their behalf'.

Digital Operational Resilience Act

On 10 May 2022, Council and European Parliament reached political agreement on the Digital Operational Resilience Act (DORA). Concerning the operational and security risks, the scope of PSD2 and DORA partly overlaps. The main difference consists in the fact that the 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 for the financial sector (set out by the DORA-Regulation and accompanying DORA-Directive) was formally adopted in November 2022. It enters into force in 2023 and will take effect as of 17 January 2025. This new framework will apply to all categories of PSPs regulated under PSD2: credit institutions, payment institutions (including certain small payment institutions which may have been exempted from certain supervision and authorisation requirements pursuant to Article 32(1) PSD2), account information service providers which only offer account information services and are exempted from certain supervision and authorisation requirements pursuant to Article 33(1) PSD2 and e-money institutions, including those that may be exempted in accordance with Article 9(1) of EMD2.

The new rules on digital operational resilience for the above 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 of Article 95 PSD2 (management of operational and security risks) PSD2 applies comprehensively (i.e. to all types of security risk), but those PSD2 rules will be without prejudice to the full application of ICT risk management requirements laid out in Chapter II DORA (which would apply instead)[279]. 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 reported under DORA, irrespective of whether such incidents are ICT-related or not[280].

Anti-Money Laundering Directive

Directive 2018/843 on anti-money laundering and countering the financing of terrorism (AMLDV) entered into force on 9 July 2018. AML/CFT provisions are complementary to PSD2. PSPs are considered "obliged entities" and as such fall within the scope of AMLDV. One prominent issue raised by market participants as regards the interplay between the PSD2 and the AMLDV is the inclusion of AISPs within the scope of the AML/CFT requirements. The EBA reiterated that while AISPs are obliged entities under the AMLD and that they are therefore required to comply with the AMLD requirements, they can adjust, on a risk-sensitive basis, the extent of some of the measures they take to comply[281]. The EBA also

---

279 Amendment to Article 95 PSD2 introduced by Article 7(2)(a) of DORA-Directive.
280 Recital 21a of DORA-Regulation.
281 Paragraph 149 of the EBA Report on the future AML/CFT framework in the EU.

reiterated that while Article 33 of PSD2 exempts AISPs from certain requirements set out in PSD2, including the requirement to provide a description of their AML/CFT internal control mechanisms when applying for registration, this does not affect the fact that AISPs are obliged entities under the AMLD. This has also been confirmed by the EC in Q&A 4712.

The evaluation did not identify issues in PSD2 with regard to coherence with AMLDV.

Settlement Finality Directive

Directive 1998/26/EC on settlement finality in payment and securities settlement systems (SFD) aims to reduce systemic risk arising from the insolvency of participants in payment and securities settlement systems. The Directive lays down the categories of participants that are eligible to participate directly in an SFD-designated system and thus benefit from the protection offered by the SFD.

EMIs and PIs are currently not eligible direct participants for payment systems which are designated under the SFD. In line with this, Article 35(2)(a) of PSD2 carves out such designated payment systems from the obligation to have proportional, objective and non-discriminatory access rules. The two pieces of legislation are thus coherent with each other, but the consequence is lack of level playing field between banks and non-bank PSPs. In the absence of a harmonised solution at EU level, some Member States have introduced national solutions that allow EMIs and PIs direct participation in payment systems, provided that certain criteria are fulfilled. This situation has led to level playing field issues between Member States and fragmentation of the European retail payment market.

Markets in Crypto-assets Regulation

The Regulation on Markets in Crypto-assets (MiCA) which regulates the issuance of crypto-assets, including the so-called stablecoins, is expected to be formally adopted by the co-legislators in Q1/Q2 2023[282]. Amongst crypto assets, MiCA includes two types of stablecoins: 1) Asset-Referenced Tokens (ARTs), which are defined as crypto-assets that are not electronic money and that purport to maintain a stable value by referencing any other value or right or combination, including one or more official currencies and 2) E-Money Tokens (EMTs), which is a type of crypto asset that purports to maintain a stable value by referencing the value of one official currency. One key difference between ARTs and EMTs is that the latter is e-money, and hence payment transactions with EMTs are automatically covered by the provisions of the PSD2 and EMD2 which apply to e-money.

Whilst MiCA regulates the issuance of crypto-assets, it does not regulate the provision of payment services by the issuers of these assets (crypto-asset service providers - CASPs). When CASPs offer payment services as part of their crypto asset services, except for E-

[282] Provisional political agreement was reached on the 30 June 2022 followed by endorsement by COREPER on 5 October and the ECON on 10 October 2022.

Money Tokens as explained above, the CASP is either to be authorised both under MiCA and PSD2 or has to appoint a PSP that is authorised under PSD2.

In this context, the EBA stressed the need to pay close attention to the treatment of EMTs, the issuers of which are required to conform to requirements under the EMD2, and for which it may need to be clarified that they fall under the scope of the definition of "*funds*" for the purposes of PSD2[283].

General Data Protection Regulation (GDPR)

Article 94(1) PSD2 clarifies that any processing of personal data, including the provision of information about the processing, for the purposes of the PSD2, shall be carried out in accordance with the GDPR and with Regulation (EU) 2018/1725.

The GDPR coming into force has raised questions for market stakeholders as to how ASPSPs and TPPs should apply the GDPR requirements in the context of the PSD2 framework regarding processing of payment account data.

In December 2020, the European Data Protection Board adopted Guidelines with the aim of providing further guidance on data protection aspects in the context of the PSD2, in particular on the relationship between relevant provisions on the GDPR and the PSD2. The main focus of these guidelines is on the processing of personal data by AISPs and PISPs. It also addresses different notions of explicit consent under the PSD2 and the GDPR, the processing of 'silent party data', the processing of special categories of personal data by PISPs and AISPs, and the application of the main data protection principles set forth by the GDPR, including data minimisation, transparency, accountability, and security measures.

In the context of the EDPB's consultation on these guidelines, various categories of PSPs regulated under PSD2 and representing the European payments industry have expressed several concerns[284]. In particular regarding processing of special categories of data, silent party data and minimization. Views expressed by several market stakeholders in the targeted consultation referred to the same issues. In this regard, many respondents expressed the need for a better coherence between PSD2 and GDPR, with some suggesting the removal of Article 94(2), as GDPR would still apply.

The EBA in its Advice has also reported that the EDPB guidelines have not eased market stakeholders' understanding as to how ASPSPs and TPPs should apply the GDPR requirements in the context of the PSD2 framework regarding processing of payment account data. The VVA study recommends only one minor clarification to make sure that Article 94 also applies to AISPs, which fall under the exemption of Article 33.

---

[283] EBA Advice (EBA/Op/2022/06), p. 111 et seq.

[284] European Banking Federation, Joint Payments Industry Letter on Final EDPB Guidelines PSD2 GDPR Interplay, January 2022

It can be concluded that certain provisions in the PSD2 should be reviewed in light of EU data protection rules.

Other legislative acts

- Regulation (EU) 2021/1230 on cross-border payments (CBPR2): This Regulation lays down rules on cross-border payments and on the transparency of currency conversion charges within the Union. However, it does not cover payment transactions from the EU to third countries (one-leg out), which are only regulated in the PSD2. Feedback from the public consultation as regards a possible extension of the transparency provisions on currency conversion charges in the CBPR2 to one-leg out transactions in PSD2 is balanced (40 respondents are in favour, including BEUC, and 35 against a disclosure requirement of currency conversion costs for one-leg out transactions). The vast majority of negative replies come from credit institutions, claiming that EU payment service providers may not be able to guarantee conversion rates for certain currencies and opposing "the extra-territorial application of EU rules".

- 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 (SEPA-Regulation): This Regulation lays down rules for credit transfer and direct debit transactions denominated in euro within the Union where both the payer's payment service provider and the payee's payment service provider are located in the Union, or where the sole payment service provider (PSP) involved in the payment transaction is located in the Union. The evaluation did not identify any coherence issues with the SEPA Regulation.

4.2 How did the EU intervention make a difference and to whom?

Summary assessment: The evaluation shows that the subsidiarity arguments put forward together with the PSD2 proposal are still valid. An integrated payments market could only be achieved with an EU intervention. Overall, the main benefits of market integration in terms of increased competition, consumer choice, innovation and security for payment service users have been achieved. However, cross-border payments continue to be fragmented along national borders.

The following section presents the main benefits of the EU intervention. It assesses whether the subsidiarity arguments put forward in the impact assessment of the Commissions' proposal on PSD2 were valid and whether the expected changes resulting from EU action were delivered.

The subsidiarity analysis of the Commissions' proposal on PSD2[285] assumes that an integrated EU market for electronic retail payments contributes to the aim of Article 3 TFEU

[285] SWD(2013) 288 final, p. 35.

stipulating an internal market. The benefits of market integration would include more competition between PSPs and more choice, innovation and security for payment service users, especially consumers. By its nature an integrated payments market, based on networks that reach beyond national borders, would require an EU-wide approach as the applicable principles, rules, processes and standards have to be consistent across all Member States in order to achieve legal certainty and a level playing field for all market participants. The alternative to an EU-wide approach would be a system of multilateral or bilateral agreements the complexity and costs of which would be prohibitive as compared to legislation at European level. For these reasons, intervention at EU level was considered to comply with the subsidiarity principle[286].

According to the VVA/CEPS study[287], there is consensus among a wide range of stakeholders that the PSD2 represents a major step forward for the payments industry, enabling the emergence of new business models and facilitating market access for non-bank payment providers. The ability of payment service providers to access a single market for payments in the EU, and to passport their services across that market[288] was a significant factor for the development of the payments market in Europe. Therefore, PSD2 had an overall positive impact on competition. This was also echoed by respondents to the targeted consultation, where 77% agreed that the EU payment market is more competitive than it was 5 years ago.

The VVA/CEPS study found that PSD2 has contributed to a certain extent to the development of cross-border payments within the EU. However, there are significant national differences in the implementation and interpretation of PSD2, which has led to regulatory arbitrage[289]. This was also reflected in the feedback on the targeted consultation, where less than half of the respondents (43%) agreed that PSD2 has contributed to the development of cross-border payments within the EU.

Furthermore, according to the VVA/CEPS study, 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 between ASPSPs and TPPs.

The VVA/CEPS study further outlines that 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 are based on the sharing of payment account data such as payment initiation services (PIS) and account information services (AIS). Several public

---

286 Recital 109 PSD2.

287 VVA/CEPS study, p. 94 et seq.

288 According to the EBA's 2019 Report On The Impact Of Fintech On Payment Institutions' And E-Money Institutions' Business Models, 45% of authorised institutions in the EU are using or planning to use the EU passporting system to provide cross-border services.

289 VVA/CEPS study, p. 196.

authorities noted that there already existed 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 public authorities indicated that they have received more licencing applications by AISPs and PISPs.

A majority of respondents to the public consultation find that the choice of payment services has increased over the last 5 years (70% yes – 66 replies). 66% of respondents to the targeted consultation agree that PSD2 creates an environment which stimulates innovation in payment services.

According to the VVA/CEPS study, PSD2 fostered innovation particularly in those markets that were underdeveloped in terms of innovativeness and Fintech solutions. There is less consensus about improved innovation in those payment markets that were already advanced (though unregulated at EU level) before the Directive was implemented (e.g. Nordic countries).

The VVA/CEPS study also outlines that PSD2 triggered innovation in incumbents' legacy business models. For example, the emergence of E-money firms offering fast payments pushed traditional banks to move into the instant payment space. Another example of innovation can be seen as a result of Open Banking provisions in PSD2 (despite the difficulties in accessing payment account data held by ASPSPs) which have resulted in APIs being able to provide much richer data sources when compared to the previous regulatory context where screen scraping was used. Open Banking requirements unlocked the possibility to combine analytics and machine learning techniques to understand payment patterns and derive some key performance indicators from bank data.

Moreover, PSD2 has improved the general level of the security of payment transactions through the implementation of SCA. This was echoed by respondents to the public consultation. Respondents to the public consultation feel that digital payments have become more secure (42 replies, 64%), and that SCA has helped to make digital payments safer and more secure (50 replies, 76%). 85% of respondents to the targeted consultation agree that making electronic payments is safer than before PSD2.

4.3 Is the intervention still relevant?

Summary assessment: Overall, the Directive's general and specific objectives remain largely appropriate as the needs identified at their inception remain relevant. The exception is the objective on aligning steering and charging practices across countries. This objective has been mostly achieved following the introduction of the surcharging ban, which harmonized charging and steering practices for a large share of payments in the EU. Continuing structural issues such as market concentration regarding payment schemes at EU level, regulatory divergence across Member States, and lagging enforcement mean that the needs for more effective competition, reducing the fragmentation of payments markets, and achieving more consistency in the application of the Directive remain relevant. New market developments such as the emergence of new business models, or the growing role of technical service

providers like pass-through wallets foreground the need for improving clarity on the regulatory status of all payment service providers. Meanwhile, new forms of fraud reaffirm the need of increasing consumer protection. As a result, the objectives accompanying these needs remain appropriate.

The relevance section assesses whether and to what extent the objectives of PSD2 are still relevant. Objectives are considered to remain appropriate if they continue to address the need to which they are linked, even when that need has evolved. The analysis thus examines the relationship between the needs identified at the time of the PSD2's inception, and in relation to which its objectives were formulated, and the evolution of those needs over the time of its implementation.

As previously noted (*c.f. section 2.1.*), the needs stem from three problem drivers:

1) ***Market failures***: a fragmented market for innovative solutions (*Need 1*), and competition issues in some payment areas (*Need 2*);
2) ***Regulatory and supervisory gaps***: diverse charging practices between Member States (*Need 3*), legal vacuum for certain PSPs (*Need 4*), the inconsistent application of PSD 2 (*Need 5*), and diverging supervisory and licencing rules and practices (*Need 6*);
3) ***Lagging consumer protection*** (*Need 7*).

As illustrated in Figure 1 on the PSD2 intervention logic (cf. 2.1.), these needs link to general and specific policy objectives that were set up to address them, and which can be mapped as follows:

1) *Needs 1 and 2 (**Market failures)** link to General Objective 1* (ensuring a level playing field between between incumbent and new providers of card, internet and mobile payments), *General Objective 2* (to increase the efficiency, transparency and choice of payment instruments for payment service users) and *General Objective 3* (to facilitate the provision of card, internet and mobile payment services across borders within the EU by ensuring a Single Market for payments); in addition, *Need 1* is covered by *Specific Objective 1* (to address standardisation and interoperability gaps for card, internet and mobile payments), and *Need 2* by *Specific Objective 2* (to eliminate hurdles for competition, in particular for card and internet payments);

2) *Needs 3, 4, 5 and 6 (**Regulatory and supervisory gaps)** link also to General Objective 3* (to facilitate the provision of card, internet and mobile payment services across borders within the EU by ensuring a Single Market for payments), and to *General Objective 4* (to create an environment which helps innovative payment services to reach a broader market); in addition, *Need 3* is accompanied by *Specific Objective 3* (to better align charging and steering practices for payment services across the EU), *Need 4* has the accompanying *Specific Objective 4* (to ensure that emerging payment service providers are covered by the regulatory

framework governing retail payments in the EU), and *Needs 5* and *6* the accompanying *Specific Objective 5* (to improve the consistent application of the legislative framework across Member States and to better align licensing and supervisory rules for payment services across Member States);

3) *Need 7 (**Lagging consumer protection**) links to General Objective 5* (to ensure a high-level protection for PSUs across all Member States of the EU) and is also covered by *Specific Objective 6* (to protect the consumer interests in view of regulatory changes in the card business and to extend the regulatory protection to new channels and innovative payment services).

To assess to what extent the objectives of the PSD2 remain relevant, the section considers whether and how the needs outlined at the inception of PSD2 have evolved and might change in the future. More precisely, needs underpinning PSD2 and informing its objectives are affected by continuing and new market developments, policy priorities, and expected future trends ('Better Regulation toolbox' Tool #47).

In this regard, market developments at the inception of PSD2 and which remain significant include: 1) the fragmentation of the EU payment services market; 2) limited market penetration by innovative payment solutions; 3) ineffective competition in certain areas of payments; 4) diverging licensing and supervisory practices; 5) the increasing use of cashless and contactless payments; and 6) diverging fraud rates between Member States and emergence of new types of fraud.

In addition, a number of new market trends have unfolded between the adoption of PSD2 and mid-2022 with implications in terms of its underlying needs. These include: 1) the emergence of 'premium' APIs, API aggregation, and 'license-as-a-service'; 2) the growth of digital wallet services, confirming the entry of BigTechs into the payments market; and 3) the growth in account-to-account payment services (notably instant payments).

The needs underlying PSD2 may also be affected by certain policy priorities and regulatory interventions, namely: 1) the prioritization of improving access of non-bank PSPs (EMIs/PIs) to payment systems, as indicated in both the EU and Eurosystem's Retail Payment Strategies[290]; 2) the political endorsement of pan-European payment solutions (such as the industry-led European Payments Initiative[291]); and 3) legislative proposal on instant

[290] Cf. 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, p.25; ECB (2021), The Eurosystem's retail payments strategy, p.4.

[291] European Payments Initiative, which comprises 31 European banks/credit institutions and 2 third-party acquirers, aims to create a new pan-European payment solution leveraging Instant Payments and cards. Cf. About - European Payments Initiative (epicompany.eu).

payments[292]. It is expected that without further policy interventions the market developments outlined above will continue.

Furthermore, a number of expected future trends might also impact relevance, namely: 1) the introduction of a digital Euro; 2) the use of crypto assets as a means of payment; 3) the unification[293] of POS and online payments in commerce; and 4) the continuing shift of commerce to digital marketplaces and platforms.

The extent and ways in which these developments affect the relevance of each of the seven needs and their accompanying general and specific objectives is discussed below. Overall, the needs underpinning the PSD2 continue to be relevant today, with the exception of the need to harmonise charging and steering practices across Member States (Need 3). This has largely been addressed by the introduction of the surcharging ban, which has harmonized charging and steering practices for a large share of payments in the EU. As a result, the objectives of PSD2 remain to a large extent appropriate, with the exception of the objective on steering charging practices across countries which has to a large extent been achieved.

1) Problem driver 1: Market failures

*Needs stemming from this problem driver (1 and 2) link to General Objective 1 (*ensuring a level playing field between between incumbent and new providers of card, internet and mobile payments), *General Objective 2* (to increase the efficiency, transparency and choice of payment instruments for payment service users) and *General Objective 3* (to facilitate the provision of card, internet and mobile payment services across borders within the EU by ensuring a Single Market for payments). In addition, each need links to an accompanying specific objective.

Need 1: Resolve the fragmented market for innovative payment solutions

Need 1 refers to the issue of low inter-operability across EU Member States for card, online and mobile payments, impeding service providers from scaling up innovative, safe, and easy-to-use payment services. Need 1 has *the accompanying* ***specific objective 1*** *'to address standardisation and interoperability gaps for card, internet and mobile payments'*

Need 1 remains *highly relevant* in a continuing market context where standardisation and inter-operability between different solutions remains lacking (with most domestic payment

[292] Proposal for a Regulation Of The European Parliament And Of The Council amending Regulations (EU) No 260/2012 and (EU) 2021/1230 as regards instant credit transfers in euro, COM(2022) 546 final, 26.10.2022.

[293] "Unified commerce" refers to the integration of the various channels of a retailer with the aim of ensuring that both payment methods as well as data collection are synchronized within the limits of the data protection rules.

schemes not working across borders)[294]. This need remains *relevant* also in a context in which, on the one hand, the growth in account-to-account payments along the lines of domestic schemes may entrench payments within national borders, and, on the other hand, PSD2-enabled PIS lack effective access to payment accounts data.

Meanwhile, this need is expected to become *less relevant* following three main policy developments, although it will still take some time for their effects to materialize. First, the political support given to the development of pan-European payment solutions that can be widely used and compete with the established international card schemes. In this regard, in 2019, the European Commission and the European Central Bank welcomed and gave their political support to the European Payments Initiative (EPI) launched by 16 Eurozone banks[295]. The creation of such pan-European payment solutions (e.g. also the interoperability initiatives developed by the European Mobile Payment Systems Association)[296] is expected to ease cross-border payments and facilitate scaling up of innovative payment solutions built around this proposition. Also, the legislative proposal on instant payments adopted by the Commission on 26 October 2022 will address the current fragmentation of instant-based payment solutions in the EU. In this respect, it should be noted, however, that the actual number of payments completed through instant payments have lagged, standing at 13% of all euro credit transfers at the end of 2022[297]. Other developments likely to decrease the relevance of this need include (a) the initiative for the standardisation and interoperability of the European Payments Council's QR-code of SEPA credit transfers initiated via mobile[298] and (b) the take-up of instant payments within the SEPA Instant framework, as this solution is designed as a pan-European solution, thus not facing cross-border interoperability issues.

The relevance of Need 1 may also change with expected future trends. Notably, it will likely *decrease* if competitive alternatives to established payment methods are developed. These may include the ECB-issued CBDC (which is expected to facilitate pan-European, resilient, fast, and inexpensive payments)[299], PSD2-enabled PIS having effective access to payment accounts data beyond domestic payment schemes, and the regulated use of crypto-assets as a means of payment following implementation of the Markets in Crypto-Assets (MiCA) Regulation[300]. The MiCA framework should reduce fragmentation of payment solutions as business solutions built around asset-referenced tokens and e-money tokens should easily

---

294 COM(2020) 592, A Retail Payments Strategy for the EU.

295 European Commission, European payments: The European Commission welcomes the initiative by a group of 16 banks to launch a European payments initiative (EPI), News Announcement, 2 July 2020; ECB, ECB welcomes initiative to launch new European payment solution, press release, 2 July 2020.

296 EMPSA - European Mobile Payment Systems Association.

297 European Payments Council, SCT Inst scheme – where are we now and where are we heading?

298 European Payments Council, The final version of the "Standardisation of QR-codes for MSCTs", 17 June 22.

299 ECB, Central bank digital currencies: a monetary anchor for digital innovation, Speech by Fabio Panetta, Member of the Executive Board of the ECB, at the Elcano Royal Institute, Madrid, 5 November 2021.

300 Proposal for a Regulation Of The European Parliament And Of The Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM(2020) 593 final, 24.9.2020.

scale across the EU. However, in the case where some solutions such as stablecoins may come to be developed and offered within the context of closed-loop systems, it is likely that the fragmentation entailed with such systems prolong this need. Finally, as PSD2-enabled PISs become fully cross-border by design, ensuring effective access to payment accounts data will promote an integrated market.

Need 2: More effective competition in certain payment areas

Need 2 links to several restrictive business rules and practices which have meant that competition in certain areas of card and online payments has not always been effective. Need 2 is linked to the ***specific objective 2*** *of addressing competition distortions*.

Need 2 remains *highly relevant* in the context of a continuing market trend where competition by innovative payment solutions remains limited vis-à-vis traditional solutions, i.e. cash and card payments. Even if, as previously noted, cash payments represent a decreasing share of payments at the POS and P2P both in terms of the number of transactions and in terms of value, in 2022 cash and card combined still represented 93% share of payment instruments used at POS/P2P, while payment cards were the most commonly used payment instrument for making online purchases[301]. While consumers are progressively using e-payment solutions including mobile payments (particularly in P2P transactions), their share of total transactions has only grown slowly (cf. section 3.2).

Need 2 remains *relevant* also in the context of continuing trends such as the persistent fragmentation of the EU retail payments market, where limited inter-operability between domestic card and account-to-account schemes (including instant payment solutions) means that the market remains dependent on a small number of international card schemes for cross border payments in shops and e-commerce (see 3.2.). Also, information asymmetries persist in certain areas of internet payments, with consumers often unaware of the different merchant transaction fees associated with different payments methods. As consumers are unaware of the costs behind each payment method, this can lead to a sub-optimal choice for more expensive payment methods (credit card vs. account-to-account), increasing transaction costs for merchants and hence consumer prices. In contrast, new market developments like the increase in domestic account-to-account schemes (see 3.2) can constitute competitive challenge to PSD PISs, as the latter may not benefit from the same network effects, recognisability and promotion as the former, when these are owned by established ASPSPs.

2) Problem driver 2: Regulatory and supervisory gaps

Needs stemming from this problem driver 3, 4, 5 and 6 link also to General Objective 3 (to facilitate the provision of card, internet and mobile payment services across borders within the EU by ensuring a Single Market for payments), and to General Objective 4 (to create an

[301] ECB (2022), Study on the payment attitudes of consumers in the euro area (SPACE), December 2022.

environment which helps innovative payment services to reach a broader market). In addition, each need links to an accompanying specific objective.

Need 3: Harmonization of charging practices between Member States

Need 3 arose from the fact that, prior to PSD2, half of the Member States allowed surcharging while it was forbidden in the other half, which led to a situation where it was often unclear for consumers whether merchants could surcharge them, especially in cross-border e-commerce, as merchants located in a country where surcharging was allowed could offer products and services in countries where it was not and surcharge consumers. Furthermore, surcharging, which was intended to allow merchants to steer consumers to the most cost-efficient payment methods, was being exploited by some retailers, who applied excessive surcharges to increase their revenues.

Need 3 was accompanied by the **specific objective 3** 'to better align charging and steering practices for payment services across the EU'.

A surcharge is a charge from merchants to consumers that is added on top of the requested price for goods and services when a certain payment method (usually a card) is used by the consumer. One of the reasons for surcharging is to direct consumers to cheaper (from the merchant's perspective) or more efficient payment instruments, hence fostering competition between alternative payment methods.

Article 62(3) to (5) PSD2 govern charging practices. The rule is that payees are allowed to, *inter alia*, request charges from payers in order to steer them towards the use of specific payment instruments (surcharging). Any charges applied shall not exceed the direct costs borne by the payee for the use of the specific payment instrument [Article 62(3)].

However, payees are prevented from requesting charges for the use of payment instruments for which interchange fees are regulated under Chapter II of Regulation (EU) 2015/751, i.e., for consumer debit and credit cards issued under four-party card schemes, and for those payment services to which Regulation (EU) No 260/2012[302] (the 'SEPA Regulation') applies, i.e., credit transfer and direct debit transactions denominated in euro within the Union [Article 62(4)].

Finally, Member States may (further) prohibit or limit the right of the payee to request charges taking into account the need to encourage competition and promote the use of efficient payment instruments [Article 62(5)].[303] There is no evidence of any official

[302] 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.

[303] 15 Member States have made use of the option to further ban surcharging.

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[304].

The surcharging ban has harmonized charging and steering practices for a large share of payments in the EU[305]. Yet not all types of payments are covered by it, and some divergence still exists as a result. Considering that 95% of card payments are subject to the surcharging ban, national divergences affect only a very small part of the payment market[306]. In the rare occasion that surcharges are applied in a Member State, the surcharge is no longer allowed [Article 62(3)] to go beyond 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.

Some stakeholders suggest that some card schemes, in particular international schemes, have increased scheme fees to make up for the lost revenues from regulated interchange fees and that, due to the ban of surcharging for interchange regulated card payment transactions, merchants have been incorporating the extra costs of accepting such cards in their retail prices. However, there is no evidence that interchange fees are no longer the main component of merchant service charges nor that the surcharging ban based on the capping of interchange fees led to a situation where merchants are now accepting consumer cards without the ability to surcharge while incurring higher scheme fees.

The surcharging ban covering those payment services to which the SEPA Regulation applies is limited to credit transfer and direct debit payment transactions denominated in euro, and not in other EU currencies, given the currency scope of the SEPA Regulation itself. The need of *Harmonization of charging practices between Member States* is still relevant as the regulatory gap between the different currencies persists for SEPA regulated instruments.

Need 4: Regulating the status of all payments service providers

Need 4 addresses the issue of a variety of innovative services primarily offering payment initiation services (PIS) and account information services (AIS) that were previously unregulated.

Need 4 has the accompanying ***specific objective 4*** *of ensuring that emerging payment service providers are covered by the regulatory framework governing retail payments in the EU*.

---

[304] In the 10 Member States covered in the in-depth analysis, namely Belgium, France, Germany, Ireland, Italy, Lithuania, Netherlands, Poland, Spain, and Sweden.

[305] European Commission, Directorate-General for Competition, Study on the application of the Interchange Fee Regulation, Final Report, 2020.

[306] European Commission, Payment Services Directive and Interchange fees Regulation: frequently asked questions, Memo, 24 July 2013.

Whilst PSD2 has brought into scope previously unregulated PSPs means that the need to regulate all PSPs has been addressed, new market developments mean that clarifying the regulatory status of market players in the payment market remains *relevant*.

First, as large technology firms enter the payment services market, for example, by offering their own stable coin, or by providing digital wallet solutions, they may operate outside, or within the exemptions, of PSD2[307]. Notably, as Bigtechs develop their payment solutions in the EU market, their ability to benefit from network effects may distort the level playing field. Yet, as their role in the payment market grows, further clarifications on scope and supervision may be warranted to ensure harmonised application of the rules and to avoid their circumvention of regulation and supervision.

Second, the need to regulate the status of all PSPs remains relevant in the context of a number of new market developments such as the emergence of premium APIs and "license-as-service" business models, where licensed and unlicensed parties competing with one another stresses a need to go beyond the 'basic access' covered under PSD2. Also, the emergence of API aggregators, which offer a paid-for alternative to a PSD2 API standard, would under the *proviso* of effective access to payment data/functioning PSD 2 API, increase the cost of market entry for new payment solutions, as new entrants must choose between costly implementation of proprietary connections with different APIs of varying quality, use fallback customer interfaces or pay service costs to an aggregator.

Need 5: More consistency in the application of PSD2

Need 5 links to the main problems in consistency of the interpretation and enforcement of PSD across Member States, including (but not limited to) the interpretation and application of exclusions and exemptions.

Need 5 has the accompanying ***specific objective 5*** *of improving the consistent application of PSD2 across Member States and better aligning licensing and supervisory rules.*

This need remains highly *relevant* in a context where slow and/or ineffective enforcement underpins many of the limitations to progress on the PSD2's objectives analysed under the 'effectiveness' section. Somewhat counterintuitively, responses to questions in the targeted consultation that focused explicitly on enforcement suggest that stakeholders (notably PSPs and NCAs) consider PSD2 provisions on this matter to be adequate, with respondents mostly agreeing that NCAs are sufficiently empowered to ensure the correct application of PSD2 (64 against 18 who disagree) and impose penalties where needed (61/15). However, inconsistencies and/or insufficiency related to supervision and/ or enforcement were also frequently mentioned in many stakeholders' constributions across various topics. This was particularly the case in relation to the access to customer account data held by ASPSPs, with

[307] Although in the former case, providers offering stable coin- based payment solutions should fall under the scope of MiCA, in addition to PSD2.

many TPPs noting insufficient enforcement with regard to the implementation of data access interfaces. The same issue was also raised in the EBA in its Advice, as noted previously.

The need also remains relevant considering how the definition of "payment account" continues to be differently interpreted across the EU. In this regard, the EBA observed how different interpretations have led to uncertainty regarding the different types of account data which can be accessed by AISPs and PISPs across the EU, with, for instance, AISPs accessing credit card data in some jurisdictions but not in others.

Moreover, guidance and responses to regulatory questions from national supervisors still vary across Member States resulting in interpretational and market transparency issues for new market actors, incumbents and users. Notably, in this regard, the EBA has noted in its Advice that the application of the requirements on the 'limited network exclusion' under Article 3(k) of PSD2 diverge significantly between Member States, creating opportunities for regulatory arbitrage. Similarly, the EBA has identified issues related to the interpretation and application of the 'commercial agent' exclusion under Article 3(b) of PSD2. Particularly, the EBA notes that, considering that commercial agents are typically defined in national civil law, which can diverge from one Member State to another, lack of clarity in the provisions regarding the specific use-cases that are intended to be covered by the exclusion hampers consistency.

Finally, this need remains relevant in the context of unharmonised application of the methods for calculation of own funds of PI across the EU under Article 9 of PSD2. More precisely, the EBA notes a divergence in the application of the requirement on who should be responsible for choosing the method for the calculation of own funds where, at times, PIs were allowed to choose the method, potentially leading to regulatory arbitrage.

Need 6: Harmonization of licensing and supervisory rules and practices

Need 6 addresses the issue of the wide margin of discretion in the interpretation of PSD1, leading to diverging licensing and supervisory practices in Member States.

Need 6 is also covered by ***specific objective 5*** *of improving the consistent application of PSD2 across Member States and better aligning licensing and supervisory rules*.

This need *remains highly relevant* as divergence in licensing and supervisory rules and practices across Member States has remained since the launch of the PSD2. Indeed, responses submitted in the targeted consultation revealed that a majority of stakeholders find that both the PSD2 authorisation and supervisory frameworks are not applied consistently across the EU (60% and 76%, respectively, of those who responded to these questions). Relatedly, some respondents to the targeted consultation found that PSD2 leads to regulatory arbitrage (21%).

More precisely, the need for further harmonizing supervisory practices remains relevant in the context of persistent divergence in NCAs' assessment of whether cross-border activities carried out by PIs and EMIs using agents or distributors fall under the ROE or the FPS. As noted in the EBA's Advice, such divergences can lead to disagreements between NCAs

and/or between NCAs and PSPs as to the applicable regulatory requirements and supervisory powers. Moreover, as the EBA also notes, NCAs have taken divergent approaches to how passporting notifications should be treated in the case of "triangular passporting", creating challenges to the supervision of activities carried out in the host Member State (including from an AML/CFT perspective).

This need also continues to be relevant with regard to the divergence across Member States in their approaches to the authorisation of payment services linked to a payment account, and notably in the authorization requirements for PIs, as previously noted (*cf. 4.1.1 Obj. 3*).

Finally, both the VVA/CEPS study and the EBA Advice have reported PSPs' concerns regarding differences in the duration of the application process across national authorities. While Article 12 of PSD2 prescribes that national competent authorities shall inform the applicant whether an authorisation is granted or refused within 3 months, the EBA has flagged concerns by applicants in relation to the duration of the authorisation process in some Member States where, at times, it may exceed one year. Besides making such activities difficult, one effect is the scope for regulatory arbitrage, as firms can 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).

3) Problem driver 3: Lagging consumer protection

Need 7: Increased consumer protection

Need 7 refers to the security risks co-emerging with the development and adoption of new payment solutions, increased digitalisation, and the growing popularity of e-commerce.

Need 7 links to ***general objective 5*** *of ensuring a high level of protection for users across all Member States.* Additionally, it is addressed by ***specific objective 6*** *of protecting consumer interests and extending protection to new channels and innovative payment services*.

This need remains *relevant* within a continuing market context of an increased use of cashless and contactless payment methods, and security of payment remains one of the main priorities for consumers when choosing a payment method. EBA's preliminary analysis of payment fraud data[308] and the assessment of the SCA migration data for e-commerce card-based payment transactions[309] suggested that fraud rates are significantly lower for payment transactions where SCA is applied compared to those where SCA is not applied.

[308] EBA, Discussion Paper On EBA's Preliminary Observations on Selected Payment Fraud Data Under PSD2, as Reported by the Industry, EBA/DP/2022/01, 17 January 2022.

[309] EBA, Report On The Data Provided By Payment Service Providers On Their Readiness To Apply Strong Customer Authentication For E- Commerce Card- Based Payment Transactions, EBA/REP/2021/16, 2021.

Notwithstanding, as also reported by the EBA[310], fraud rates in H2 2020 still differed between the EEA countries and across the selected payment instruments[311]. In addition, the emergence of new types of fraud (including social engineering, phishing, malware)[312] means that the need for customer protection remains relevant.

Furthermore, this need remains *relevant* in the context of three new market developments. First, in the context of the emergence of premium APIs and "license-as-a-service" providers, consumers may not be able to differentiate between licensed and unlicensed parties, and thus might not be aware of the enhanced risks entailed with non-PSD2 licensed entities (e.g. fraud or misappropriation of funds, lower technical security standards and less transparency on costs). Second, one remark emerging in the VVA/CEPS study concerns how safety of consumer's accounts and data might become more difficult to ensure in a context where ASPSPs will not always have sight on which TPPs ultimately use the customer data or initiate a payment when transmitted through an aggregator.

Finally, the need for increased consumer protection is likely to remain *relevant* with regard to the expected future development of asset-referenced tokens and e-money tokens to become (partial) money substitutes and the adoption of crypto-assets as a means of payment, particularly given the highly technical nature and market volatility related to crypto-assets.

As a result of new payment services sometimes falling outside of the scope of PSD2, and the unharmonised authentication methods to access account information, **both general objective 5 and specific objective 6 therefore remain relevant.**

5. WHAT ARE THE CONCLUSIONS AND LESSONS LEARNED?

Based on the analysis presented in the previous sections, this section presents the conclusions of the evaluation of the PSD2 framework. While it is beyond the scope of the evaluation to provide any policy conclusions or follow-up action, the section highlights the main lessons learned, which inform the proposal for revision as well as the impact assessment.

---

310 EBA/DP/2022/01.

311 More precisely, for credit transfers (H22020), the share of fraud in the volume of payments ranged from a rate of 0.0002 % to 0.0027 % (with the median fraud rate at 0.0005 %) across the EEA countries included in the sample. Fraud as share of payment value ranged from 0.0003 % to 0.0025 % (with a median fraud rate of 0.0010 %). For card payments as reported by issuers, the share of fraud in the total volume of payments ranged from 0.0031 % to 0.0309 % (while the median fraud rate was 0.0103%). The share of fraud in the total card payment value ranged from 0.0043 % to 0.0572 % (median fraud rate was 0.0191 %). (EBA/DP/2022/01).

312 European Payments Council, 2022 Payment Threats and Fraud Trends, EPC183-22, 23/11/2022.

5.1. Conclusions

The evaluation analysis has shown that, despite certain shortcomings, the current PSD2 framework has enabled progress towards its objectives, while being relatively efficient with regard to its costs, and delivering EU added value.

More specifically, the PSD2 framework has been particularly effective with regard to its goal of increasing the efficiency, transparency and choice of payment instruments for payment service users (general objective 2). While the evaluation has identified some scope for improvement (including more transparent information on PSPs' business information and charges), it has also been demonstrated that the PSD2 framework has contributed to increase the choice of payment solutions available to PSUs, including by harmonizing steering and charging practices and facilitating the passporting of services by TPPs across the EU.

The PSD2 has also been mostly successful regarding its consumer protection objectives (general objective 5). Particularly, provisions on SCA have significantly reduced the risk of fraudulent transactions for consumers, even if the inherently adaptive nature of fraud calls for attention to new practices that have developed since (e.g. social engineering fraud). Another point of caution concerns the technological bias towards mobile devices which can lead to the exclusion of some consumer groups from access to some services (e.g. remote electronic payments, online access to payment accounts), and their associated customer protection.

The conclusions of the evaluation are however less positive with regard to progress made on the market failure-related problem drivers identified in the PSD2 Impact Assessment. With regard to competition and level playing field objectives (general objective 1), the extension of the legislation's scope to cover previously unregulated market players (i.e. PISPs and AISPs) has been followed by an increase in the number of TPPs, as well as innovation in the payments market. Notwithstanding, the evaluation has identified important limitations to PSD2's effectiveness regarding this goal, most notably the persisting unbalance in the level playing field between bank and non-bank PSPs ensuing from the lack of direct access to payment systems by the latter.

Also, the goal of broadening market access for TPPs (general objective 4) has not been fully achieved by current provisions on Open Banking, mostly as a result of a fragmented landscape of variable quality APIs and unsatisfactory data sharing. In this context, ASPSPs have been concerned with the cost of developing APIs, claiming a lack of remuneration incentives. In turn, TPPs have often pointed out the lesser quality of those access interfaces provided by ASPSPs (when compared to their own user interfaces), as well as the additional costs related to connecting to different APIs. In this context, while the general view held by both ASPSPs and TPPs is against API standardization, it is noteworthy that several TPPs expressed agreement with a remuneration model for ASPSPs for services beyond the baseline as potentially leading to an improvement in data access.

However, PSD2 has also only had limited success in improving the EU cross-border payments market, as fragmentation along national lines persists, despite the appearance of

certain pan-EU payment Fintech PSPs. Accordingly, while cross-border credit transfers have been facilitated in the context of developments related to the SEPA Regulation, the market in cross-border card payments is still dominated by international card schemes, especially as interoperability between domestic account-to-account and card payment schemes remains limited.

Regarding efficiency, the cost-benefit analysis carried out by the VVA/CEPS study has identified that the largest cost items associated with the implementation of PSD2 are linked to Open Banking and in particular API-development, SCA roll-out (implementation costs and increase in transaction abandonment rates) and legal interpretation/uncertainty. However, this conclusion should be taken with caution, due to the assumptions used and the paucity of data (only two responses from banks). A large majority of credit institutions and banking associations consulted for the study considered that the costs of the PSD2 so far largely outweigh the benefits. 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. But these largely one-off costs are expected to be offset over time by recurring benefits, most of which come from the improvement of the functioning of the single market, followed by unlocked potential for innovation, and a more secure payment environment. While the costs of the PSD2 were incurred in the initial stages (i.e. substantial investment costs), the benefits – although significant – only materialise gradually, and it is therefore difficult to draw an overall conclusion regarding costs and benefits at this time, as only few years have passed since the PSD2 has been fully implemented. 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 cost reduction is overall relatively modest.

Notwithstanding, when considering efficiency, several limitations, in particular as regards the robustness of data, apply. More precisely, the efficiency analysis is based on the results of the cost-benefit analysis presented in the VVA/CEPS study on the basis of its stakeholder consultation, as well as of an analysis of the relevant literature. Evidence on the costs and benefits of PSD2 is, however, still 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, like one-off implementation costs (e.g. enabling of account data access, SCA), whereas the longer-term effects can only be estimated. Moreover, another caveat is that costs and benefits may vary between Member States. Despite these limitations in the data underlying the evaluation analysis, findings from studies and more recent surveys provide an indication of the most critical aspects, which account for the bulk of the costs arising from the implementation of the Directive.

Finally, the evaluation has shown that PSD2 has EU added value. Indeed, the subsidiarity arguments put forward together with the proposal are still valid. By its nature, an integrated payments market, based on networks that reach beyond national borders, requires an EU-wide approach as the applicable principles, rules, processes and standards have to be consistent across all Member States in order to achieve legal certainty and a level playing field for all market participants. The ability for payment service providers to access a single

market for payments in the EU, and to passport their services across that market[313] was a significant factor for the development of the payments market in Europe.

5.2. Lessons learned

The following points summarise some lessons learned in this evaluation. In line with the backward-looking character of the evaluation exercise, the lessons drawn here concern firstly the relevance of the problems and needs that were initially identified and that led to PSD2. Secondly, this evaluation also allows drawing lessons in terms of the coherence of the legislation, both internal and external. Moreover, one more general key lesson concerns also data collection, where the expectable shortage of available data related to the early stage of many innovations under scrutiny should, in the future, inform more thorough and targeted data collection, notably via the consultation strategy.

Regarding the needs identified at the inception of PSD2, and which inform the Directive's general and specific objectives, the evaluation has determined that these remain relevant, with two exceptions. First, whereas PSD2 has covered previously unregulated market players such as PISPs and AISPs, this has largely addressed the need to regulate all PSPs. Notwithstanding, market developments such as the emergence of new business models, or the growing role of technical service providers such as processors and digital wallets, have raised questions and would benefit from additional clarity regarding their regulatory status. A second exception is the objective on steering and charging practices across countries. This has been mostly achieved following the introduction of the surcharging ban, which has harmonized charging and steering practices for a large share of payments in the EU.

Continuing structural issues, such as market concentration in cross-border card payments at EU level (still largely handled by a few international card schemes), enduring divergence in the implementation and interpretation of PSD2 across Member States, and new forms of fraud mean that the needs for more effective competition, reducing the fragmentation of payments markets, and increasing consumer protection remains relevant. As a result, its accompanying objectives remain relevant as well. The growth of account-to-account payment schemes of domestic scale and still limited interoperability also confirm the need to resolve the fragmentation of the European payment market. Meanwhile, policy developments like the emergence of pan-European payment solutions, as well as expected future trends like the uptake of crypto-assets (in particular stablecoins) as a payment method or the adoption of a digital Euro, might mean that the relevance of some needs related to competition and fragmentation within the European payments market become less relevant in the future.

Regarding its coherence, the PSD2 has a high degree of internal coherence. In terms of external coherence, the evaluation has identified consistency issues between the PSD2 and

---

[313] According to the EBA report of July 2019, 45% of authorised institutions in the EU are using or planning to use the EU passporting system to provide cross-border services.

the General Data Protection Regulation (particularly with regard to the notion of explicit consent) to be addressed in the review. Moreover, lessons can also be drawn from some consistency issues between the PSD2 and other EU legislation such as the E-Money Directive, the Settlement Finality Directive, the Digital Operational Resilience Act, the Crypto Asset Markets Regulation. Notably, with regard to the coherence between PSD2 and the Settlement Finality Directive, E-money institutions and payment institutions are currently not eligible direct participants for payment systems which are designated under the SFD. In line with this, Article 35(2)(a) of PSD2 carves out such designated payment systems from the obligation to have proportional objective and non-discriminatory access rules. The two pieces of legislation are thus coherent with each other, but the consequence is a lack of level playing field between banks and non-bank PSPs. Thus, coherence does not always have a positive impact.

ANNEX 6: SCOPE OF PSD2

1. Introduction

Since PSD2 was adopted in December 2015, based on a Commission proposal of July 2013, many new payment services and solutions have evolved and new players have entered the payment market.

For example, providers of so-called e-wallets (specifically "pass-through wallets"[314]) allow for tokenisation of an issued payment instrument and its use via a mobile device to make online or contactless payments. New means of payment have developed such as e-money tokens (EMTs, a type of crypto asset). Existing players have adjusted their business model to the needs of consumers, amongst others. Players can provide both payment and other services, such as provision of "buy now pay later" services in addition to the execution of payment transactions.

This raises two issues, firstly whether the scope of PSD2 should be extended in order to cover certain new actors, and secondly whether clarifications are necessary in order to ensure a proper application of the rules. The current definitions of PSD2 regarding scope have proved on many occasions ambiguous and too general in light of the market evolution, and rules are to some extent "outdated". This applies amongst others to some existing rules on the exclusions from the framework and also for the definition of the list of payment services which are in scope.

As a result, there have been different interpretation and application practices between NCAs across the EU. Market actors are competing with each other, although some of them benefit from unjustified advantages (e.g. being treated as excluded although they should be treated as within scope); other actors face disadvantages (e.g. not allowed to benefit from the passporting rules and because of this facing barriers to market entry). In the end, an uneven level playing field may exist and consumers may face protection gaps. PSPs or TPPs might be tempted to seek authorisation and supervision in the Member State with the interpretation of the rules most favourable to them, even if this is not a Member State where they are active ("forum shopping") although article 11§3 of PSD2 requiring that 'part of the business' be carried out in the home country needs to be respected. Some stakeholders have called for extension of the scope of PSD2 to include some of these categories of providers currently outside the scope (see Annex 2).

[314] « Pass-through wallets » should be distinguished from « staged wallets » on which a balance of electronic money is stored ; issuance of a staged wallet requires a license as an Electronic Money Institution.

2. Possible changes to scope as regards technical service providers

Article 3(j) of PSD2 conditionally excludes from the scope of the Directive "technical services providers"[315]. These are essentially payment systems and infrastructures and technical service providers supporting the provision, by regulated payment service providers, of payment services. Certain consumer-facing services such as so-called 'pass-through wallets' (e.g. Apple Pay or Google Pay) are also covered by this exclusion as they do not provide a payment service per se[316]. Commission services have considered whether to amend this exclusion, for example by including some TSPs in the scope of the legal framework. The conclusion was not to do so, for a number for reasons:

- Firstly, there was no predominant view on this question in the various consultations, with very varied views among stakeholders. Consumers and other stakeholders did not raise issues regarding such service providers, including the "pass-through" wallets. There is no compelling evidence from the consultations, VVA/CEPS study or EBA Advice that their current situation outside PSD2's scope is detrimental to either users or to the payment system itself. Compelling evidence to justify extension of the scope of PSD2, with consequent significant costs for newly covered entities which would be subject for the first time to a requirement of authorisation and supervision, has not been found.

- Secondly, most of these currently excluded services and their providers (systems, schemes, infrastructures, processors etc.) are already subjected to European Central Bank/Eurosystem oversight (based on article 127§2 of the Treaty), including processors and arrangements (such as digital wallets) which are covered by the new 'PISA'[317] oversight framework of the ECB which is currently being progressively rolled-out. The ECB's oversight framework draws inspiration from the international standards adopted by the BIS's Committee on Payment and Settlement Systems (PFMI)[318]. Applying to such providers PSD2 rules and supervision requirements would risk significant overlaps with ECB oversight. The Eurosystem does not support bringing the operators of payment systems and payment schemes under an authorization and supervision regime and hence recommends not to consider those

[315] Article 3(j) excludes: "services provided by technical service providers, which support the provision of payment services, without them entering at any time into possession of the funds to be transferred, including processing and storage of data, trust and privacy protection services, data and entity authentication, information technology (IT) and communication network provision, provision and maintenance of terminals and devices used for payment services, with the exclusion of payment initiation services and account information services".

[316] These wallets store 'tokenised' payment cards in a digital wallet carried by a smart phone, but the actual payment is performed through the card scheme selected by the user, not by the wallet operator.

[317] PISA: Payment Instruments, Schemes and Arrangements. https://www.ecb.europa.eu/paym/pdf/consultations/ecb.PISApublicconsultation202111_1.en.pdf.

[318] https://www.bis.org/cpmi/publ/d101a.pdf.

activities under the PSD2 review[319]. However, since the PISA framework is not yet fully applied, this aspect will be kept under close review with a view to assessing whether an EU licensing regime is in future necessary[320].

- Thirdly, the logic of PSD2 is to regulate services provided to end-users (consumers, merchants) and not services pertaining to the operation of the payment 'rails' (the systems and infrastructures), nor services supporting the execution of payment services without being payment services themselves (payment data processing, operation of payment terminals, cloud services etc.) or services only facilitating the choice and use of a payment instrument (without carrying out the payment service itself). These services (with the exception of wallets) are largely invisible to the payment user and do not directly interact with the user. Any possible legislation for non-consumer-facing payment infrastructures would more logically belong in a separate piece of legislation, but this decision will be taken once a thorough review is carried-out of, notably, the efficiency of the ECB oversight framework.[321]

- Fourthly, the fact that entities providing services within the scope of PSD are automatically also included in the scope of the EU Anti-Money-Laundering Directive, due to a dynamic cross-linkage of the scope also pleads in favour of caution in extending the scope of PSD[322]. The cost for any such newly covered entities of implementing EU AML rules would be very significant.

However, it should be emphasised that already in PSD2, article 35 contains some provisions applicable to payment systems, as regards their access rules, without however, subjecting

---

[319] Correspondence from the Eurosystem Committee in Market Infrastructures and Payments to the European Commission, 11 January 2023.

[320] This is also in line with the review article (article 58) of the recently-published Regulation on Digital Operational Resilience (Regulation 2022/2554), which requires the Commission to assess and report to the European Parliament and the Council on the need for increased cyber resilience of payment infrastructures, which are excluded from the scope of that Regulation. See Annex 12.

[321] For comparison, in the area of securities, consumer-facing services are regulated by MiFID, while infrastructures are regulated by the Regulation on Central Securities Depositories and by the Regulation on European Market Infrastructures.

[322] AMLD scope defines "financial institutions" as being among Obliged Entities, and in the definition of "financial institutions" it includes "an undertaking other than a credit institution or an investment firm, which carries out one or more of the activities listed in points (2) to (12), (14) and (15) of Annex I to Directive 2013/36/EU of the European Parliament and of the Council [this is the Directive on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms]". Annex 1 of Directive 2013/36/EU includes as point (4) [i.e. among points (2) to (12)] "Payment services as defined in Article 4(3) of Directive 2007/64/EC [PSD1 but this reference is dynamically corrected to PSD2 with the replacement of PSD1 by PSD2]. Therefore, undertakings providing payment services in the meaning of PSD2 are defined as "financial institutions" in the meaning of AMLD and are therefore Obliged Entities for AML purposes.

such payment systems to authorisation or supervision rules. This impact assessment discusses elsewhere whether those rules should be enhanced[323].

3. Specific issues concerning pass-through wallets

Two specific interpretation issues regarding pass-through wallets have arisen in the context of PSD2 implementation:

- Does the tokenisation of an existing payment instrument in such a wallet (for example a payment card) amount to the issuance of a new payment instrument, and if so, which party issues the new tokenised payment instrument, the PSP which issued the original payment instrument, or the operator of the wallet? If the answer to the first question is yes and the answer to the second question is the operator of the wallet, then the wallet operator would already today need a PSP license. It will be clarified that unless it could be used as a standalone payment instrument that can be used to initiate a payment order independently from the underlying tokenised payment instrument (e.g. a card), the token cannot be considered as being itself a payment instrument but, rather, a 'payment application' within the meaning of Art. 2(21) of the Interchange Fee Regulation.
- Can the operator of a digital pass-through wallet carry out SCA, on behalf of the issuer of the original payment instrument, when the tokenised instrument stored in the wallet is used for a payment? Here, it will be clarified, in line with the relevant EBA Q&As[324] that this is possible, but only with an outsourcing agreement under which the original issuer retains full liability for any failure of SCA and has the right to audit and control the wallet operator's security provisions.

These clarifications should provide sufficient certainty about the status of pass-through wallets, without the need to bring them within the scope of PSD and subject them to a full licensing and supervision regime. Oversight by the ECB should be sufficient for now, but this subject will be re-evaluated in the next review of PSD.

4. Possible deletion from the scope: account information services and payment initiation services

Account information services, being information-related and not involving any payment, are heterogeneous to the other services listed in Annex 1 of PSD2, all of which involve the safeguarding or moving of funds. Entities which only carry out account information services must obtain a license as a Payment Institution, but with a lighter set of requirements than account servicing Payment Institutions. Some stakeholders have suggested that account information services might belong more appropriately in the future legislative framework on

[323] See sections 2.1.4. 2.2.4, and 6.1.4. of the impact assessment, which discuss these rules.
[324] See EBA press release of 31 January 2023.

Open Finance[325]. However, such a move could only be seriously envisaged once the legislative framework on Open Finance is known and agreed politically. A situation in which account information services would become unregulated for a certain time (for example, if they were removed from PSD2 before any new OF regime would enter into force) cannot be risked since there would be a tangible danger that AISPs would, even if only temporarily, lose their data access rights. Also, the risk of a disruptive transition to a new legal regime must be avoided for AISPs, and the transition can only be successfully managed once the final version of the Open Finance framework is known, after adoption by the co-legislators. A transfer of AIS to the OF framework is not ruled out in a future review.

Regarding PISPs, it is considered that since they initiate payment transactions rather than receiving and using data, they belong in the legal framework on payments -as providing an inherently payment service- not in the future framework on Open Finance.

5. **Other clarifications on scope**

In light of these considerations, it is proposed only to make essential clarifications on the rules on the scope of PSD2 where there are currently ambiguities, but without making significant changes to the scope (no new inclusions or exclusions of categories of service providers). This is a matter of textual clarifications in order to allow a harmonised application across the EU and to allow for a proper coverage of relevant services and actors. If one would not clarify the scope of PSD2, PSD2 would still allow for different application practices. Consumers would continue to be exposed to unsupervised parties which should be supervised and do not comply with PSD2´s rules e.g. on framework contracts, amongst others. An uneven level playing field would remain.

In order to remedy this, the following textual clarifications are foreseen:

a. **Clarify the definitions of payment services in annex I:** insert further definitions on different payment services to the legal text (currently only some payment services are defined in detail), and alongside this clarify, where necessary, further related definitions (e.g. payment instruments in the context of issuance and payment accounts in the context of the execution of payment transaction); merge definitions of related and/or separate divergent payment services where appropriate; adapt and update the wording to current market reality.

b. **Clarify some exclusions in article 3, in particular:**
   - Commercial agent: give examples of covered business cases in the relevant recital (outline the actual used cases) and provide further clarifications in the actual legal text (e.g. outline the term "commercial agent" and the term "negotiate and

[325] A legislative proposal on Open Finance, analogous to Open Banking but concerning other financial services such as insurance and investment services, is scheduled for 2023 in the Commission's 2023 Work Programme.

conclude"); where necessary mandate the European Banking Authority to develop Guidelines.

- Limited network: streamline the terms used (e.g. "professional issuer" and "premises of the issuer"), outline the geographical limits for the instrument, and mandate the European Banking Authority to amend and update its Guidelines[326]where necessary.

Furthermore, it is envisaged to textually clarify:

- The coverage of business models that are based on cooperation between a licensed entity and a non-licensed entity (e.g. for cases where the non-licensed entity obtains control over the entire business activity and in particular controls the interaction towards the consumer). It will be in particular clarified (in a recital) whether the agency framework (if the non-licensed entity acts on behalf of the licensed entity), the outsourcing framework (if the non-licensed entity supports the services provided by the licensed entity), and the actual licensing requirement (if both involved entities provided services that qualify as payment services) need to be applied.
- The confirmation of the availability of funds services (see article 65 of PSD2) will be removed from the PSD2 as this business model never took off and no provider of this service is currently licensed. The framework will be lightened and adjusted to market reality.

[326] Guidelines on the limited network exclusion under PSD2.

ANNEX 7: TECHNICAL CLARIFICATIONS AND OTHER CHANGES

The purpose of this annex is to list a number of clarifications and technical and relatively minor changes which the current initiative will bring to PSD2, many of them on the basis of responses prepared either by EBA or the European Commission to questions submitted according to the Q&A process laid down in the EBA Regulation[327]. These clarifications and technical changes fall into a number of areas (see Annex 6 above for clarifications on scope).

Definitions

The numerous different adjustments of the current provisions in PSD2 as explained in the main body of the impact assessment will be reflected in the list of definitions as well where appropriate. There will be for example updates on the definitions of 'payment accounts', 'payment instruments' and 'funds'. Beyond that there will be new definitions introduced where necessary to clarify and make it easier to apply the new rules for instance in the context of strong customer authentication (initiation and execution of payment transactions). Some rather prominent examples can be found in the following:

- Article 4(12) – 'payment accounts': clarify the functions of payment accounts as regards the execution of payment transactions and the sending and receiving of funds in light of recent ECJ rulings (C-191/17).
- Article 4(14) – 'payment instrument': specify the meaning of payment instruments in light of recent ECJ rulings (C-287/19).
- Article 4(16) – 'account information services': due to further developments in this business model, the definition has to be modified to clarify that an AIS can be provided either directly to the payment service user or be transmitted, with the user consent, to another party, for example a non-bank lender or a credit scoring agency which uses the account information to provide a credit score.
- Article 4(25) – 'funds': provide an updated understanding in line with other pieces of EU legislation (e.g. in the context of EMD provisions or the digital euro).

Surcharging

Article 62(3) to (5) of PSD2 govern charging practices. The current rule is that payees are allowed to, *inter alia*, request charges from payers in order to steer them towards the use of specific payment instruments (surcharging). However, payees are prevented from requesting charges for the use of payment instruments for which interchange fees are regulated under Chapter II of Regulation (EU) 2015/751, i.e., for consumer debit and credit cards issued under four-party card schemes, and for those payment services to which Regulation (EU) No

[327] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), article 16b.

260/2012[328] (the 'SEPA Regulation') applies, i.e., credit transfer and direct debit transactions denominated in euro within the Union (Article 62(4)). The VVA/CEPS Report concluded that the rules on charges are appropriate and had a positive impact and that there is no need for alignment of charging practices between Member States, as the surcharging ban applies to a large share of payments in the EU (95% of card payments are subject to the surcharging ban).

Reordering the provisions under Article 62(3),(4),(5) would allow to have a better systematic structure of Article 62. The ban on surcharging for consumer debit and credit cards regulated under the Interchange Fees Regulation and on credit transfers would come first, followed by the provision giving Member States' discretion to further ban surcharging and, finally, the residual provision allowing surcharging for all other cases. The surcharging ban covering those payment services to which the SEPA Regulation applies is limited to credit transfer and direct debit payment transactions denominated in euro, and not in other EU currencies, given the currency scope of the SEPA Regulation itself. Changes to be introduced on substance will therefore concern the extension of the surcharging ban to <u>all</u> credit transfers and direct debits not just to those covered by the SEPA Regulation.

<u>Application of Strong Customer Authentication and fraud beyond SCA</u>

This section provides further details about envisaged amendments to SCA and fraud prevention measures, in addition to those provided in the main impact assessment report.

The current definition of 'inherence', which, under Article 4(30) PSD2 means "something the user is" would be further clarified in view of the way innovation may contribute to payments security.

To the EBA, inherence, which includes biometrics relating to physical properties of body parts, physiological characteristics and behavioural processes created by the body, and any combination of these. The EBA, in its Advice excludes from inherence behavioural characteristics related to the environmental analysis and payment habits. To the EBA, environmental analysis and payment habits can be viewed in the light of the transaction risk analysis ('TRA') under Arts. 2 and 18 of the RTS.

There are, however, reasons to consider further specifying PSD2's definition of 'inherence' to allow the use for SCA of environmental analysis and payment habits:

- The TRA exemption is subject to cumulative conditions, notably to low 'exemption threshold values'. Hence, it is of limited scope.
- The EBA agrees that environmental analysis and payment habits contribute to improving the security of payment transactions/data

[328] 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.

The UK Financial Conduct Authority approved spending patterns as a valid inherence element for SCA.[329] The FCA considers that 'inherence' is as a characteristic attributable to a person regardless of whether it relates to a physical property of the body or a behavioural characteristic (e.g., detailed shopping patterns). Alignment of the PSD definitions of 'inherence' with the UK definition would be carefully considered, in light of the additional SCA elements and the benefits potentially stemming to PSPs, payers and payees from such harmonization.

The second set of SCA related changes concern **transaction risk analysis** monitoring. Article 18 of the RTS provides for an SCA exemption, laying down that payment service providers shall be allowed not to apply SCA where the payer initiates a remote digital payment transaction identified by the payment service provider as posing a low level of risk according to the transaction monitoring mechanisms (TMMs) referred to in Article 2 of the RTS (the 'transaction risk analysis' SCA exemption). Many stakeholders voiced in their input to the targeted consultation that the current provisions governing 'transaction risk analysis' (TRA) are insufficient as, for instance as they are perceived to include a "broad definition of risks". As a result, respondents flag that many relevant providers do not adopt TRA, because the requirements make it unattractive. Public authorities shared a similar view, noting that feedback from the market showed that the current exemption from SCA under article 18 of the RTS on the use of TRA is not used to a significant extent due to cumbersome audit and governance requirements. In addition, respondents also claimed that card issuers lack the incentive to develop TRA solutions, as they have to pay for all the respective costs, also to the benefit of other parties, such as payees. Respondents argue that the absence of a clear guideline on audit content requirements providing more detail and better definitions on risk monitoring requirements and data to share deters more PSPs/EMIs from implementing TRA, that could provide improved risk analysis/monitoring. It is necessary to design appropriate guidance and rules on the scope and the perimeter of TRA, introducing a clear guideline on audit content requirements, providing more detail and better definitions on risk monitoring requirements and data to share, and to consider allowing PSPs to report fraudulent transactions in TRA for which they are solely liable. The relevant exemption threshold values, specified in the table set out in the Annex to the RTS, which date back to 2017, and cannot be exceeded by a given transaction to fall under the TRA SCA exemption, would need to be updated.

As mentioned above, TMMs are the basis for the risk analysis exemption to the application of SCA. In order to also improve TMMs, the general requirement for PSPs to have in place TMMs would be moved from the RTS[330] to Level 1 legislation (as proposed by the EBA in its Advice)[331] in order to emphasise the political priority of this measure and its crucial

---

[329] UK Financial Conduct Authority, Policy Statement on Changes to the SCA-RTS and to the guidance in 'Payment Services and Electronic Money – Our Approach' and the Perimeter Guidance Manual, November 2021, page 26.

[330] Monitoring mechanisms are not mandated by the Directive itself, but only in Articles 2 and 18 of the RTS.

[331] Advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2), 23 June 2022, page 80.

contribution to fraud prevention. This would also serve the purpose of clarifying that TMMs concern security requirements against fraud that go beyond the protection offered by SCA, which does not currently result from the relevant provisions of the RTS that require the implementation of TMMs specifically to ensure compliance with the SCA requirements. Moving TMMs to level 1 would also allow to clarify that the obligation to implement TMMs applies not only to payment transactions but also to open banking services (in particular in the context of account information services), which also does not result from the RTS provisions on TMMs mentioned above, which focus on payment transactions. This would result in an extended scope of TMMs, further contributing to fraud prevention.

Furthermore, there is merit in the EBA's proposal to mandate it to set out the specific technical requirements related to the TMMs (e.g., ensuring that richer data points are covered by TMMs) and better definitions on risk monitoring requirements, helping stakeholders to reap the full benefits of the mechanism combating fraud.[332] TMMs would be, with fraud data sharing and awareness campaigns, the central piece of the fraud prevention arsenal. It would also be directly linked with the new liability requirements for authorised transactions because, as noted by the EBA, PSPs have little incentives to invest in effective transaction monitoring mechanisms that could mitigate the social engineering risks, because in most cases the losses are passed on to the PSUs.[333]

As mentioned above, PSPs are already required under the RTS to implement TMMs, having had to integrate it. There are, therefore, costs that have already been incurred by PSPs to comply with the requirement to adopt TMMs. It is too early to quantify potential additional implementation costs, as they would be dependent on the nature and scope of the specific technical requirements that are yet to be developed by the EBA. Potential additional costs would be weighed against the benefits in terms of broader and improved fraud prevention stemming from having more effective TMMs based, *inter alia*, on richer data points.

The fourth group of changes to SCA and fraud beyond SCA concerns the initiation of digital remote payment transactions and the requirement for PSPs to apply SCA that includes elements which dynamically link the transaction to a specific amount and a specific payee (Article 97(2) PSD2 and Article 5 RTS). There is the need to introduce a clearer definition of 'remote digital payment transactions' and define 'initiation of an digital payment transaction'. There is also the need to clarify the specific risks that are to be addressed with the dynamic linking requirements for remote transactions.

The purpose is to create a level playing field between card-based wallets and mobile initiated credit transfers at physical point of interaction ('POI') in terms of the SCA requirements with dynamic linking. The current definition of 'remote digital payment transactions' does not seem to provide an up to date and precise framework to decide whether mobile initiated credit transfers at POI (e.g., when SCA is performed online) are remote payments, requiring SCA dynamic linking. Under PSD2, remote payment transaction' means a payment

[332] *Ibid*.
[333] *Ibid*, page 82.

transaction initiated via internet or through a device that can be used for distance communication. EBA Q&A 4594[334] clarified that a "*payment transaction is remote when initiated via internet or, in case the transaction is initiated via a device, where the physical presence of the device is irrelevant for the initiation of the payment transaction*". As a result, for instance, the mere use of a mobile phone at POI would be a remote transaction, which might result in some level of ambiguity for mobile payments at POI and level playing field concerns.

The issue does not only have to do with the current definitions under PSD2, but also with the need to understand and clarify in the legal framework if dynamic linking is only meant to cater for the risks of tampering with the payee name and the specific amount of the transaction between payment initiation and authentication of (online) remote payments, or if it also addresses the additional risk of fraud more generally, such as a fraudster intercepting the communication between the PSU and the PSP, as the EBA Q&A 2020-5367[335] indicates. Q&A 2020-5367 clarifies that credit transfers at POI with online authentication require dynamic linking.

Supervision

Some of the articles of Title II of the Directive require some clarifications and updating, for example a revision of the initial capital requirements to reflect inflation, or to reflect the clarifications that were requested through the EBA Q&A tool. The most important of these clarifications are listed below:

Article 7 - initial capital: update to include the inflation rate since the first PSD1 (2007), as the PSD2 of 2015 did not make any changes. Given the fact that the majority of the data gathered and used for the PSD2 review was up until end-2021, the inflation rate of 2007-2021 (ECB's Harmonized Index of Consumer Prices[336]) is used to recalculate the initial capital ratios: 23.1%. The figures are then rounded down to the nearest ten or five (thousand). This results in the following amended initial capital figures for Annex I services:

- For the providers of service (1) to (5) an increase from 125.000 € to 150.000 €.
- For the providers of service (6) an increase from 20.000 € to 25.000 €
- For the providers of service (7) the initial capital requirements of 50.000 € does not change. The EBA's review of initial capital in its Call for Advice concludes the 50.000 € is sufficient, and providers of service (7) also require a professional indemnity insurance or comparable guarantee (art. 5(2)) next to the initial capital, which services (1) to (6) do not. There is no further evidence to suggest the 50.000 € initial capital for PISPs is too low.

[334] 2019_4594 Definition of an electronic remote payment transaction | European Banking Authority (europa.eu).
[335] 2020_5367 SCA requirements with dynamic linking for mobile initiated credit transfers (MSCTs) | European Banking Authority (europa.eu).
[336] European Central Bank's Harmonized Index of Consumer Prices (HICP), via link.

- Due to the merger of EMD and PSD2, the own funds of EMIs becomes part of the PSD2. There is no reason other than an inflation correction to change the 350 000 € initial capital requirement for EMIs (to 400.000 €) and this will be included in a new article 7 (d).

Providers of service n°8 (AISPs) are not required to hold initial capital given the limited financial risk they face and because they do not hold own funds. This is notwithstanding any business models in which the provider combines service 8 with another of Annex I's payment services. They continue to be required to hold a professional indemnity insurance or comparable guarantee (art. 5(3)).

For article 9 – own funds: an option D for E-Money Institutions will be included, and a clarification that it is the relevant competent authority that determines which method shall be applied for the calculation of own funds. This should lead to more harmonisation (NCAs mostly apply method B, method B will be flagged as being the default rule).

Article 19 - use of agents, branches or entities to which activities are outsourced: clarify situations of 'triangular passporting', by indicating that article 19(5) also applies in case a payment institution wishes to provide payment services in another Member State than its home state through an intermediary (an agent or branch) in another, third, Member State ('triangular passporting'). These clarifications should lead to a more harmonised implementation across Member States.

Product intervention powers (for EBA)

It is envisaged to include in the legislative proposal product intervention powers to the EBA. These powers would allow the EBA to prohibit temporarily the sale of certain payment products. The EBA has these powers in principle as set out in article 9 para. 5 of the EBA regulation. EBA should however act within the powers of sectoral EU legislation. Those powers need to be technically "switched on" in the relevant field before the EBA can make use of it[337]. For other EU authorities (ESMA/EIOPA), these clarifications were already provided through other pieces of EU legislation (e.g. EMIR and PRIIPS) as a result of which product intervention powers can be applied to some financial products (insurances and investment products), however not to all relevant products. In the future (from 2024 onwards), the EBA will have these powers for products under MICA. Against this background, it will be clarified that the EBA will have product intervention powers in the field of payment services as well. These powers would allow EBA to intervene altogether if there are issues for example in cases where a single credit card product (regulated payment instrument) allow payments indeed not only with classic funds, however with categories of crypto assets that are not considered as funds (in particular asset-referenced tokens).

Alignment with MiCA (Markets in Crypto Assets Regulation)

In line with the future Regulation on Markets in Crypto-Assets, it will be clarified that payment transactions using EMTs are covered (taking into account that e-money tokens are

[337] As examples, see article 69(m) and (n) of Directive 2014/65/EU.

e-money, and hence one of the categories of funds) by the relevant provisions applying to payment transactions in the PSD2, and consider any issues regarding the applicability of these to DLT-based products (i.e. in particular provisions in Title IV of PSD2).

Measures to enhance coherence with GDPR (General Data Protection Regulation)

Explicit consent

Article 94(2) PSD2 states that "PSPs shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user". Article 4(11) GDPR defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". The parallel use of explicit consent in both legal acts has led to the question of whether "explicit consent" as mentioned in PSD2 should be construed in the same way as explicit consent under GDPR. The EDPB has clarified in its guidelines[338] that explicit consent pursuant to Article 94(2) PSD2 should be regarded as an additional requirement of a contractual nature in relation to the access to and subsequently processing and storage of personal data for the purpose of providing payment services and is therefore not the same as explicit consent under the GDPR. Legal certainty will be provided by introducing clarification on explicit consent in Articles 65, 66, 67 and 94 PSD2 in line with the EDPB guidelines.

Silent Party Data

The access to account data by AISPs and PISPs in the context of Articles 66 and 67 PSD2 has raised concerns about the processing of "silent party data". Silent party data is personal data concerning a data subject who is not the user of a specific PSP, which is processed by that PSP for the performance of a contract with a PSU. The EDPB guidelines have clarified that, in line with Article 6 (1)(f) GDPR, the legitimate interest of a controller or a third party to perform the contract with the PSU can constitute a lawful basis for the processing of silent party data by PISPs and AISPs in the context of the provision of payment services under the PSD2[339]. However, it has also stated that "*the necessity to process personal data of the silent party is limited and determined by the reasonable expectations of these data subjects*"[340]. Hence, in order to ensure legal certainty, a new legal basis in PSD on the processing of silent parties will therefore be included (in Art. 66 and 67).

Processing of special categories of data

The processing of special categories of personal data (e.g. revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, etc.) is prohibited under the GDPR[341], subject to the exceptions set out in Article 9(2) GDPR. These

[338] EDPB Guidelines 06/2020 on the interplay of PSD2 and GDPR (paragraph 36).
[339] Ibid., paragraph 48.
[340] Ibid.
[341] Article 9(1).

exceptions include cases where the data subject has given explicit consent and/or the processing is necessary for reasons of substantial public interest based on Union or national law. To provide legal certainty in situation where payment service provision could include processing of special categories of personal data, a new provision in PSD will be included related to substantial public interest to address cases where processing of special categories is necessary in the context of PSD.

ANNEX 8: INTEGRATION OF THE E-MONEY DIRECTIVE 2 INTO PSD2

1. Background

The second Electronic Money Directive (EMD2) contains the rules on authorisation and supervision of E-Money Institutions (EMIs), while PSD2 contains the rules on authorisation and supervision of Payment Institutions (PIs), and establishes the rights and obligations of the parties with regard to payment transactions executed by the three categories of PSPs recognised by the Directive (credit institutions, e-money institutions and payment institutions).

As payment transactions using e-money (transfers of e-money units) are already regulated to a very large extent by PSD2, the legal framework applicable to EMIs and PIs is already reasonably consistent. However, the licensing requirements (in particular initial capital and ongoing capital) and some key basic concepts governing the e-money business (such as issuance of e-money, e-money distribution and redeemability) are quite distinct, as compared to the services provided by payment institutions. However, as concluded by the EBA in its Advice, supervision authorities have experienced practical difficulties in clearly delineating the two regimes, and in distinguishing e-money products/services from payment services offered by payment institutions[342]. This has led to concerns about regulatory arbitrage and unlevel playing field, as well as issues with the circumvention of the requirements of EMD2 whereby some institution issuing electronic money, taking advantage of the similarity between payment services and electronic money services, apply for authorisation as a PI.

This experience acquired by applying both frameworks in parallel is now sufficient to move forward with the merger[343]. The merger of the existing Electronic Money Directive into PSD2 will be an opportunity to address these concerns and challenges with regard to delineating between the two legal frameworks, in particular at the licensing stage.

In addition to that, the merger will also be an opportunity to ensure a higher degree of harmonisation, simplification and consistent application of the legal requirements for PIs and EMIs, preventing regulatory arbitrage, ensuring a level playing field and a future-proof legal framework.

---

[342] See Paras 97 to 123 of the EBA's response to the Commission's Call for Advice.

[343] See thereto the Commission's report on the implementation and impact of Directive 2009/110/EC in particular on the application of prudential requirements for E-Money Institutions of 25 January 2018 on page 7: "*A future revision of the Directive and its merger with the revised Payment Services Directive would require further analysis. It seems appropriate to consider such steps only after Member States and stakeholders will have been able to gather experience with the adapted framework following the adoption of PSD2, which will also have an impact on e-money institutions.*"

There is a significant number of entities affected by these challenges: there are 267 E-Money Institutions and 758 Payment Institutions licensed in the EU [344].

This simplification exercise is overall supported by a majority of stakeholders in the feedback to the public consultations, in particular the targeted consultation responses[345], the VVA study[346] and the EBA response[347] to the Commission´s call for advice. There are however some concerns raised regarding a complete "absorption" of the e-money concept – these concerns are raised amongst others due to the relevance of the e-money concept for the MICA regulation and the historically grown market with its long-standing agreements among the involved parties.

2. Description of possible available scenarios/options

The baseline scenario would amount to doing nothing, no simplification exercise, no efficiency improvements. The baseline scenario includes a technical "codification" exercise amounting to copying the existing EMD provisions into PSD, however leaving all the provisions basically as they are. Beyond the baseline scenario, there are two different options on how to integrate the current EMD2 framework into PSD: 1) complete "absorption" of the concept of e-money into the PSD; 2) a middle ground solution, whereby the specificities of the E-money business are preserved, where justified, but the licensing regime is as harmonised as far as possible with the regime applicable to payment institutions.

3. Discussion of possible scenarios/options

a. In the baseline scenario, the challenges regarding a consistent application, regulatory arbitrage, and future proof legal framework would persist. There would be continued challenges in delineating the services at licensing level, in other words: a lack of effectiveness would remain. In terms of efficiency, the market actors, including NCAs, would continue to spend time and resources in finding the right approach for the application of the existing set of rules. As regards coherence, this option would also be sub-optimal, as one could argue that the two legal frameworks could be considered as inconsistent. Therefore, this option is rejected.

b. A complete integration[348] would amount to abandoning the whole concept of e-money and related specificities, and covering the activities currently considered as issuance of e-money by the existing set of payment services under PSD2. In terms of effectiveness, there would be no challenges regarding delineation between the two regimes any longer. It would however mean that legitimate differences and specificities of e-money business could no longer be

---

[344] See thereto an overview in VVA study on page 34 and 35 and the EBA´s register https://www.eba.europa.eu/risk-analysis-and-data/register-payment-electronic-money-institutions-under-PSD2.
[345] See thereto annex 2, stakeholder consultation, under "Title 1: subject matter, scope and definitions".
[346] See there on page 19.
[347] See therein number 97 onwards.
[348] See thereto no. 110 of the EBA´s response to the call for advice.

addressed, for instance as regards a necessary consumer protection due to higher initial capital requirements for the issuance of e-money as compared with the payment services which PIs are allowed to offer. In terms of efficiency, market actors including NCAs would be released from the burdensome exercise of delineating between the two regimes. As regards coherence, taking into account that MICA has just been adopted and that it establishes that one of the categories of crypto-assets that it regulates (E-Money tokens) are also e-money and should be regulated accordingly (i.e. according to the E-Money Directive) , a simple absorption of the E-money regime would be incoherent and require a complete overhaul of the recently-adopted rules for licensing and conduct of business requirements for E-Money Tokens. Therefore, this option is rejected.

c. an intermediate approach, with the two frameworks brought together in the same directive, and harmonised to the extent possible. In particular, this option would:

- more clearly delineate the distinguishing features of e-money products/services and services offered by payment institutions, so as to improve legal clarity whilst adequately addressing the risks (i.e. consumer protection).

- include electronic money related services in as large a sense as possible to the existing payment services;

- align the supervisory requirements such as those related to authorisation process, initial capital/own funds and safeguarding, while leaving still room for e-money specificities (e.g. possibly continue to require higher initial capital for the issuance of e-money, and an additional buffer for the calculation of own funds);

- clarify the nature and applicable rules for distributors of e-money products, so as to ensure a consistent approach with the rules applicable to agents of PIs.

As regards effectiveness, this intermediary approach would lead to considerable simplification of the rules to be applied (see below in the next section). In terms of efficiency, the costs and resources by market actors including NCAs in dispensing efforts to differentiate between the two frameworks would be minimized. In terms of coherence, this would be consistent with the future MICA Regulation. To preserve the technological neutrality of the regime applicable to various categories of e-money, it would not be advisable to have different requirements applicable to e-money tokens (DLT-based e-money) and other forms of e-money (non-DLT-based). Therefore, this option is to be retained.

4. Illustration of envisaged changes based on the preferred option

Examples of the specific changes envisaged based on the preferred intermediate option are for example:

- Currently there are two kinds of institutions, payment institutions and e-money institutions. Due to the simplification exercise there will be just one category, the payment institutions only (no e-money institutions any longer).
- The issuance of e-money will still be considered as a licensed activity (new dedicated service in an annex to the framework further specifying the regulated services in the framework).
- A definition of e-money as a key concept remains, as a distinct category of funds, and no changes to the definition of e-money itself is deemed necessary. However, the key distinguishing features (a claim on the issuer, redeemable at par, not bearing interest, etc) are to be spelled out and clarified in a separate provision.
- Furthermore, the distinguishing features between e-money and payment services will be spelled out more properly. The difference between funds accepted by a payment institution to be held in a payment account for the purpose of making payment transactions, and e-money issued by an E-money institution (then by the payment institution) will be that whilst the funds received for the purpose of issuing e-money remain under the full control of the e-money issuer and are the property of the e-money issuer, funds held in a payment account by a payment institution remain the property of the payment service user. The payment service user can withdraw them or place payment orders for the funds to be transferred (meaning for payment transactions to be executed); these payment orders do not however have be placed upfront, or in a specified period. This will still continue to depend on the business model of the payment institution.
- Higher initial capital will still remain (and adjusted due to inflation).
- The role and responsibilities of entities involved in the "distribution" of e-money will be clarified, amongst others the role of so called distributors will be defined and clarified that they act on behalf of the payment institution in order to distribute e-money.

The envisaged changes to PSD2 resulting from the integration of EMD2 should reduce the overall complexity of the coexistence of the two legal frameworks and bring clarity in the legal requirements/supervisory regime. It is also one of the specific initiatives announced in the Commission's 2020's Retail Payments Strategy.

4. Impacts

This measure should lead to savings for PSPs, in so far as there would no longer be a need to obtain a new license for a Payment Institution desiring to carry out e-money activity and vice versa. As PIs and EMIs are both non-bank types of Payment Service Providers, this measure will be complementary with the measures described in the main report to make the playing field between banks and non-bank PSPs more level. A reduction in new licensing applications, and the greater clarity on the distinction between e-money and payment institution activity, should reduce the resource burden on national supervisors.

ANNEX 9: ACCESS TO CASH

1. INTRODUCTION

The use of cash has been declining in the last years. Most noticeably, ECB data[349] for the euro area shows that, in 2022, cash was used in 59% of POS transactions, significantly down from 72% in 2019[350], and 79% in 2016[351]. As noted previously, the COVID-19 pandemic accelerated this trend, with contactless (including mobile) payments and digital wallets representing a larger share of total payments (cf. 1.1. and Annex 5, 3.2.).

Despite this decline, cash is still the means of payment which is most used at POS and P2P proximity payments[352]. Consumers are still attached to it, as they, appreciate its widespread acceptability, its ease of use, immediate settlement feature, as well as (perceived) safety and anonymity[353]. There are furthermore circumstances in which consumers tend to prefer cash to digital means of payments, for instance, when making low value payments (in small shops, such as a bakery or café), and it is often more widely used in rural areas. Beyond that, cash is the main means of payment accessible and/or used by certain groups such as unbanked, under-banked and offline consumers[354]. In this context where cash provides consumers with an alternative to digital means of payment, improved cash availability is therefore in consumers' interest.

There are however important differences among Member States regarding the usage of cash. Accordingly, in the Member States with the highest rates of usage of cash at POS (Malta, Slovenia and Austria) cash represented around 70% of all payments, whereas in those with the lowest rates (Netherlands and Finland) cash represented only 20% of all POS transactions[355].

Cash can be obtained in different ways, inter alia, via cash withdrawals in bank branches, via banks' ATMs, via non-bank ATM deployers and via retailers when for instance paying with payment cards (so called "cash-back services"). In average in the EU, a downward trend in the availability of ATMs and branches offering cash services can be observed[356], affecting the

---

349 ECB, Study on the payment attitudes of consumers in the euro area (SPACE), 2022.

350 ECB, Study on the payment attitudes of consumers in the euro area (SPACE), 2020.

351 ECB, Survey on the use of cash by households (SUCH), 2017.

352 ECB, Study on the payment attitudes of consumers in the euro area (SPACE), 2022.

353 ECB, Study on New Digital Payment Methods, March 2022.

354 Ibid., p.12. As understood in this study, consumers in this group present different reasons for being unbanked, underbanked and/or offline. The main reason usually related to unfavourable life circumstances (such as no steady income, not in charge of finances, personal bankruptcy), emotional barriers (distrust of banks, reluctance to use the internet and digital banking tools, negative banking experiences in the past) and functional barriers (the lack of technical skills). Often, this is also a matter of age, with older people and women being more used to traditional payment methods such as cash.

355 See thereto ECB´s Study on the payment attitudes of consumers in the euro area (SPACE) – 2022 (europa.eu) and the Final report of the Euro Legal Tender Expert Group (ELTEG).

356 See thereto ECB´s Study on the payment attitudes of consumers in the euro area (europa.eu).

availability of cash in both rural and urban areas. However, the situation is very heterogeneous across Member States, with this reduction sometimes offset by alternative means of access to cash (notably via post offices and "cash-back" services provided by retailers) in some Member States (Austria, Germany, Greece, Italy, Luxembourg, Slovakia, Slovenia, France, Malta) but not in others (Belgium, Cyprus, Spain, Finland, Ireland, Latvia, Lithuania, Netherlands).

Work is currently under way in the Commission on a draft legislative proposal on the legal tender of cash, which will include provisions on access to and acceptance of cash, as the two key elements related to legal tender. This draft legislative proposal figures in the Commission Work Programme for 2023 and is intended to be presented in parallel to a legislative proposal laying down the legal framework for the digital euro.

2. CURRENT PSD2 PROVISIONS ON CASH DISTRIBUTION

One of the eight types of payment services listed in Annex 1 of PSD2, for which a license as a PSP is necessary, is "*Services enabling cash withdrawals from a payment account as well as all the operations required for operating a payment account*." However, among the exclusions to PSD2 (in article 3) is "*services where cash is provided by the payee to the payer as part of a payment transaction following an explicit request by the payment service user just before the execution of the payment transaction through a payment for the purchase of goods or services".* This means that a retailer may provide cash to a customer in association with a purchase without having a PSP license, but (in the absence of a PSP license) may not provide cash only, i.e. without a purchase. A retailer which is acting as an agent for a Payment Institution may distribute cash and receive cash on behalf of the PI to its customers, and certain PIs in the EU have started to use this model[357].

The distribution of cash via ATM machines in general requires a license as a PSP. But there is an exclusion from PSD2 for certain "independent" ATM machine operators, with specific conditions and nevertheless imposing certain transparency requirements on those ATM operators[358]. Determination of which ATM networks are covered by that exclusion, and also enforcement of the price transparency requirements on such ATM operators, has proven challenging.

[357] For example, Nickel in France and Belgium.

[358] Article 3 (Exclusions), (o) : « cash withdrawal services offered by means of ATM by providers, acting on behalf of one or more card issuers, which are not a party to the framework contract with the customer withdrawing money from a payment account, on condition that those providers do not conduct other payment services as referred to in Annex I. Nevertheless, the customer shall be provided with the information on any withdrawal charges referred to in Articles 45, 48, 49 and 59 before carrying out the withdrawal as well as on receipt of the cash at the end of the transaction after withdrawal. »

3. ENVISAGED MEASURES

In line with the Commission's intention to present measures facilitating access to cash, and without prejudice to the contents of the Commission's draft legislative proposal on the legal tender of cash which is in preparation, it is envisaged to clarify and streamline the provisions in PSD regarding cash distribution.

Firstly, regarding physical shops, it is envisaged to allow them to offer a cash withdrawal service from a payment account held by a PSP, in the absence of a purchase by a customer, without having a PSP license or being an agent of a Payment Institution. This could be associated with the application of a cap, to be further specified but which could be in the range of 50-100 euro, and an obligation to disclose fees charged, if any. This service would be provided by retailers exclusively on a voluntary basis and would obviously depend on the availability of cash on the merchant's premises.

Secondly, the exclusion of certain types of ATM operators ("independent" ATM operators) has proven difficult to apply due to its ambiguity. This could be resolved by replacing the concept of independent ATM operators by ATM operators which do not service payment accounts. To bring them within scope, a registration regime without licensing, with an adapted set of requirements should be applied, to ensure an adequate level of regulation.

Since in all such cases, there may be a charge for cash withdrawals, transparency on fees is important, and Member States would be obliged to have penalties in place for ATM operators or other cash distributors which breach the requirement for transparency on fees.

4. IMPACTS

The impact of these measures should be to contribute to improving consumer confidence in payments and to mitigate the identified problem in these areas. It should have a particularly high impact in rural areas with few ATMs. It could also have a positive environmental impact if it prevents consumers needing to travel long to a location with an ATM in order to obtain cash.

The cost to merchants would be limited to the cost of transparency requirements about this measure. There would be no obligation on them to maintain a provision of cash, and cash distribution would be subject to availability of cash in the shop.

ANNEX 10: USER RIGHTS MEASURES

1. PROBLEMS IDENTIFIED

In the area of user protection with regard to PSPs, the public consultations have shown a number of specific instances in which users would appreciate improvement to their rights or protection when making payments:

- *Name of payee on account statements*

PSD2 includes a requirement for PSPs to provide the payer with a reference enabling the payer to identify each payment transaction and, where appropriate, information relating to the payee (Article 57). This information must be provided on paper or on another durable medium. PSPs comply with this obligation by citing the legal name of the payee on a payment account statement but not necessarily the commercial trade name, if different[359]. Article 57 does not lay down whether the legal name or commercial name should be used on statements. This can cause confusion among users, who may not recognise the name which appears on the statement and incorrectly suspect a fraudulent transaction or on the contrary miss a fraudulent transaction. Indeed, the current opacity makes it more difficult for consumers to spot unauthorized and/or fraudulent transactions, as pointed out by EBA in its Advice. This measure, recommended by the ERPB[360], is keenly requested by consumer organisations.

- *Insufficient transparency of fees for ATM usage*

When withdrawing cash from an ATM, different fees may apply depending on whether the ATM is owned by the customer's bank or not. Consumers often have to pay external withdrawal fees when using an ATM that is not owned by their bank or is a member of that bank's network. Failure to provide this information means that the consumer cannot compare the different applicable fees.

- *Blockage of funds for an excessive amount or duration*

When a payment card is used for a payment of an uncertain amount (for example at a petrol station, a hotel or a car rental), funds are normally blocked on the card by the payer's PSP after consent has been given by the payer and is unavailable for use until released. Blocked funds are unavailable to the user for spending until released, which can cause financial difficulties. In the targeted consultation, out of 67 responses only 26 respondents think that Article 75 (which regulates the blockage of funds) is adequate as opposed to 41 respondents (61%) who think the provision is not adequate. Article 75 provides that funds must be unblocked "without undue delay after receipt of the information about the exact amount of the payment transaction and at the latest immediately after receipt of the payment order"; however, "undue delay" is not defined. Furthermore, evidence received by EBA and through the public consultation show that the blocked funds may be disproportionate or unreasonably

[359] For example, "Brussels Property Management sprl" as opposed to "Hilton".
[360] Final report of the ERPB working group on transparency for retail payments end-users (europa.eu).

high. Another related issue, which brings further disadvantages to consumers, concerns the different practices regarding the timing for the release of unused blocked funds, which could, according to feedback received through the public consultation, take up to several weeks or even require an additional action in the form of an explicit request from the payer. In many such cases, the consumer contacts the payee, e.g. gas station, but is told to contact his/her bank. When contacting the bank, the consumer is often told that the bank cannot release the funds until the payee asks it to.

- *Insufficient information on currency charges and execution time with international operations outside the EEA*

PSD2 requires transparency of charges for single payment transactions and for payment transactions covered by a framework contract. However, these requirements do not explicitly refer to the foreign exchange margin, which is the mark-up that payment service providers usually apply for transactions involving currency conversion. Whilst transparency obligations for the estimated total amount and applicable currency conversion charges are included in the cross-border payments Regulation[361] (CBPR2) for intra-EU credit transfers (with the exception of the requirement to express the currency conversion as a percentage mark-up over the latest available euro foreign exchange reference rates issued by the ECB), they do not cover remittance transactions (intra-EU or to third countries) or cross-border credit transfers involving countries outside the EU (either the country where the payer or the payee is located/has its payment account), so-called "one-leg out transactions". When currency conversion is necessary, these costs are often an important share of the total costs[362]. Regarding international transactions (outside the EU/EEA), without full transparency, it is hard for consumers to compare those charges with those of other providers and to make an informed decision; consequently, they may choose a provider which is not the best provider for them. The recipient in the third country may thus receive less funds than could be the case. Promoting competition and reducing the level of fees for international credit transfers and remittances is one of the objectives of the G20 Roadmap on cross-border payments[363]. In addition, under the current Directive the requirement for PSPs to inform the payment service user about an estimate of the maximum execution time is not applicable to such transactions either.

- *SCA is often not accessible for people with disabilities and other disfavoured persons*

PSD2, being technology neutral, does not prescribe a specific technical means of complying with SCA, leaving it for PSPs to choose the authentication methods or devices to be used by their customers. It seems that some PSPs' authentication solutions might still not fully cater for the needs and situations of some categories of consumers, despite EBA's guidance on the elements of SCA that may comply with the legal requirements under PSD2 and in the RTS.[364]

---

[361] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R1230.
[362] https://remittanceprices.worldbank.org/.
[363] G20 Roadmap for Enhancing Cross-border Payments, p. 8.
[364] European Banking Authority (EBA-Op-2019-06) Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2, June 2019

Many respondents to the targeted consultation launched in 2022 by the Commission (cf. Annex 2) mention the negative impact that the current approach to SCA and the respective authentication methods have had on some groups of society in vulnerable situations (such as persons with disabilities, the elderly, or those that do not have access to digital channels/devices etc.), which might lead to increased financial exclusion of such groups. BEUC, the European Consumer Organisation, notes in its contribution to the Commission's consultation that *"a significant number of consumers do not want to use smartphones for online banking. This can be for several reasons: a) consumers do not own a smartphone; b) they cannot operate a smartphone; c) their smartphone does not accept the required app; d) for security concerns or; e) for concerns over their privacy"*, concluding that "*the PSD2 does not address this widely held consumer concern*."[365] This position is also expressed in the EBA Advice'[366]. The Commission has also received several Questions and Petitions via the European Parliament and numerous consumer complaints on the same issues.

2. ENVISAGED MEASURES

To remedy these identified problems, a package of targeted improvements to user information and rights in the respective areas is envisaged, containing the following measures:

i. Provide for both legal and commercial trade name of payee on account statements

This would involve an obligation for PSPs to provide the commercial trade name of the payee on payment account statements, which would be very effective to increase legal certainty[367] in relation to the information provided by the payment service provider to the customer identifying the payee (merchant). It would also help consumers to better recognize the identity of the merchant and to detect unauthorized and/or fraudulent transactions visible on payment account statements[368].

This would be achieved via a clarification in Article 57 to ensure that PSPs provide on payment account statements the information needed to unambiguously identify the payee, including a reference to the payee's commercial trade name. This would create legal certainty compared to the current wording in PSD2 and would make it easier for consumers to spot unauthorised or fraudulent payment transactions. The legal name of the merchant could be additionally provided if required for any other purpose.

In this context it can be noted that in June 2022, the Euro Retail Payments Board (ERPB) endorsed a set of recommendations for retail payment end-users, including a recommendation to also include the commercial trade name in payment account statements. According to a

---

[365] Bureau Européen Des Unions De Consommateurs, Review of the Payments Services Directive 2, BEUC recommendations, pp. 18 and 19.
[366] EBA/Op/2022/06), pp. 83-84.
[367] The legal interpretation of the term "*information relating to the payee*" is subject to a request for a preliminary ruling (Case C-351/21 lodged on 4 June 2021, *ZG v Beobank SA*).
[368] The lack of transparency for retail PSUs and inability to identify unauthorised and/or fraudulent transactions was also highlighted by the EBA (Point 261 EBA/Op/2022/06).

survey conducted by the ERPB[369], in general, national legislation allows the commercial trade name to be used in account statements, even when a legal entity name might also be mandated, or used even if not mandated. Some national legal requirements might present obstacles to the inclusion of the commercial trade name in account statements, while one card scheme forbids it based on national law. Nonetheless, in general, scheme rules do not present obstacles to the inclusion of the commercial trade name, while some actively encourage payees to use the name by which the customer would know them. However, these recommendations are not legally binding, which is why consumer associations (BEUC), public authorities, the ECB and the EBA advocate for legislative amendments to the PSD2 for reasons of legal certainty.

The ERBP recommendations, accompanied by an ERPB impact assessment, are expected to be fully implemented by industry by mid-2024. It can be assumed that these recommendations have already been fully implemented by the time the PSD changes come into force. If this is the case, only minor non-recurring implementation costs should be generated for PSPs by this approach.

ii. Improve transparency of fees for ATM usage

This would include a clarification of the transparency requirements for PSPs related to ATM withdrawals. PSPs would be required to disclose all domestic ATM withdrawal fees in the different situations where (i) the ATM belongs to the PSP or the PSPs network; (ii) the ATM belongs to another network with whom the PSP has an agreement; (iii) the ATM belongs to an independent ATM deployer.

This would increase the transparency of ATM charges towards the consumer and make it easier for consumers to compare ATM charges with those from other providers and to be able to make an informed decision. It would also ensure the smooth application of the principle of equality of charges between domestic and cross-border euro payments[370], as the consumer would be able to better assess, based on this information, whether fees were lawfully levied in a Member State other than where the consumer has the payment account. This option, which is only a specification of existing transparency provisions in PSD2, would only incur minor costs for PSPs (programming the ATM to show the costs before confirmation of the operation). Fee documentation would also have to be changed, on their websites and on any paper documentation that would be available to payment services users. It is assumed that payment services providers regularly update (annually) their price information documentation and this measure can be implemented in such a periodic update. However, there will be an IT cost for the update of information on the payment services providers' websites and their internal IT systems.

iii. Improve transparency on currency charges and execution time for 'one-leg-out operations'

---

[369] Implementation of the recommendations on transparency for retail payments end-users - impact assessment (europa.eu).
[370] Article 3(1) of Regulation (EU) 2021/1230 on cross-border payments in the Union.

For payment transactions (credit transfers and money remittance transactions) within the EU and from the EEA to a third country, this would include improved information requirements on currency conversion with an obligation for PSPs in the EEA to include an estimate of the total currency conversion charges up-front, based on the mark-up of a reference exchange rate, which could be for instance the ECB rate, for transactions in euro, or the relevant Central Bank rate, for other currencies. Furthermore, this option would require the payer's PSP in the EEA to inform its payer about the estimated execution time of the transfer with the payee's PSP located outside the EEA. This would improve transparency in international transactions, which is important for consumers to compare estimated currency conversion fees and execution times with other providers and to make an informed decision.

It would in turn promote competition and reduce the costs for international credit transfers and remittances, which is one of the objectives of the G20 Roadmap of 2020 on cross-border payments[371]. This option would also be coherent with the enhanced transparency provisions applicable for cross-border credit transfers within the EU introduced by the Cross-Border Payments Regulation. It would also address the arguments put forward during the consultation by the banking sector, which may not be able to guarantee exchange rates for certain exotic currencies, by limiting the transparency provision to an estimation. Unlike for transactions with the EU, payment service providers would be obliged to provide an estimated execution time but would not be held liable for the execution of the transaction within the specified time period.

Regarding payment services providers, fee documentation would have to be changed that would be available to payment services users. There will be a limited IT cost for the update of information on the PSPs' websites and their internal IT systems.

iv. Improve rules concerning blockage of funds

This would include a legal obligation for the payee (merchant) to inform its PSP about the exact amount of the payment transaction immediately after the service or goods have been delivered to the payer. Under PSD2 there is only a legal obligation on the payer's PSP to release the excess amount without undue delay, but there is no deadline for the payee to inform its PSP.

There would also be a requirement that the amount of the funds blocked by the payer's payment service provider has to be proportionate in view of the exact amount of the payment transaction which can reasonably be expected.

This would be very effective to ensure a reasonable blocked amount and faster pay-out of the excess blocked funds to the benefit of the consumer. The clarification that the merchant would be obliged to notify the final amount to his/her bank immediately would not imply any significant costs. However, Member States would have to designate a national authority responsible for ensuring compliance by the payee which may lead to enforcement costs for supervisors.

---

[371] G20 Roadmap for Enhancing Cross-border Payments, p. 8.

v. Improve the accessibility of SCA to persons with disabilities and other persons with difficulties to use SCA

A general requirement is envisaged for PSPs when designing authentication solutions to ensure that all types of clients, including persons with disabilities, elderly persons and those with low digital skills, have adapted means to make payments subject to SCA (e-payments), and that the methods offered to PSUs to perform SCA are not dependent on one single technology, device or mechanism. Voice recognition and the use of card readers, for example, could play a role in this respect. This requirement would be coherent with and complement the accessibility requirements of the European Accessibility Act, in full coherence with it. [372] Requiring PSPs to take into account the needs of customers with disabilities elderly people and those who do not have access to digital channels or devices, when designing authentication solutions (e.g., voice recognition or card readers), would improve financial inclusion of such groups of society and better protection of them from fraud, in particular when it comes to the use of remote digital payment transactions and online access to payment accounts as fundamental financial services.

3. IMPACTS

The combined impact of these measures should be to contribute to improving consumer confidence in payments and to mitigate the identified problem in this area, at relatively limited cost to PSPs.

Regarding the measure to improve the ability of persons with disabilities and other such persons to use SCA, the costs of this measure to PSPs would depend very much on their decision about how much internal resources to devote to developing such measures; PSPs could be expected to pool resources on this and not act individually. The benefits of this measure in terms of SCA public acceptance are noteworthy, and respond to the legitimate concerns of some consumer associations, NGOs etc.

[372] Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services.

ANNEX 11: EXPLANATORY NOTE ON OPEN BANKING

1. INTRODUCTION

The annex aims to complement the evaluation report as regards Open Banking. It presents indicators chosen to perform the analysis, stakeholder sentiment towards Open Banking, it provides some insight into the UK market on Open Banking and presents tentative conclusions on whether Open Banking has delivered on its potential.

2. WHAT IS OPEN BANKING IN PSD2?

Open Banking services regulated under PSD2 can be either account information services (AIS) or payment initiation services (PIS). AIS providers and PIS providers are collectively called Third Party Providers (TPPs). AIS can provide a user with aggregated and/or analysed information on the basis of their payment accounts, helping users to manage their finances or enabling users to receive a service, based on this data, from another service provider (accountant, auditor, credit scoring bureau etc.). PIS are account-to-account, non-card-based payments and can be found in e-commerce as one of the payment methods offered by merchants. AIS and PIS both require the consent of the user (PSU) to access the payment account data. Access, storage and use is limited to the data needed to perform the service requested by the PSU. AIS and PIS can also be combined e.g. by using an analysis performed on the basis of AIS in order to perform a better PIS. AIS data can, for instance, be particularly useful to help providers of PIS (PISPs) assess the risk of a payment initiated eventually not being executed.

Below are some illustrations of various Open Banking scenarios, complementary to the illustrations of more simple ones in §2.1.2 of the main impact assessment report.

Figure 1 Payment Initiation Service (Illustration Banco de Portugal)

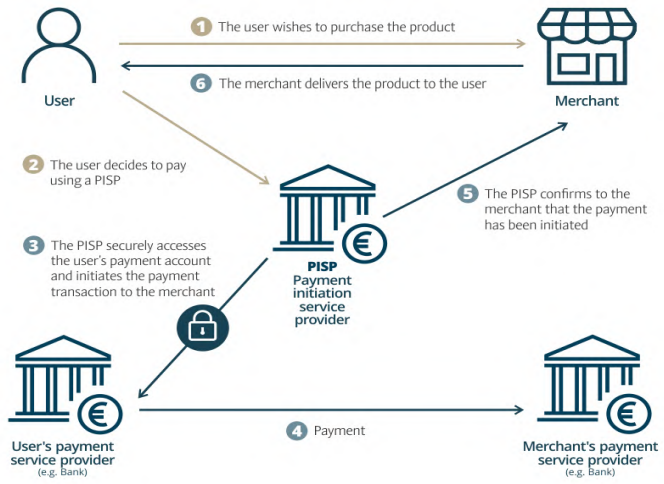


Figure 2 OB case with an aggregator (TSP or TPP)

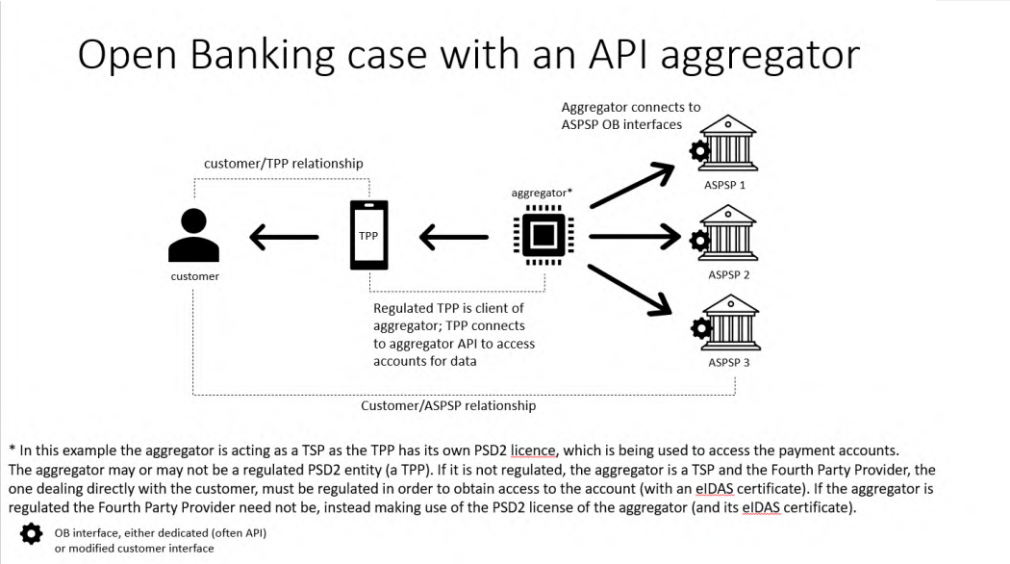
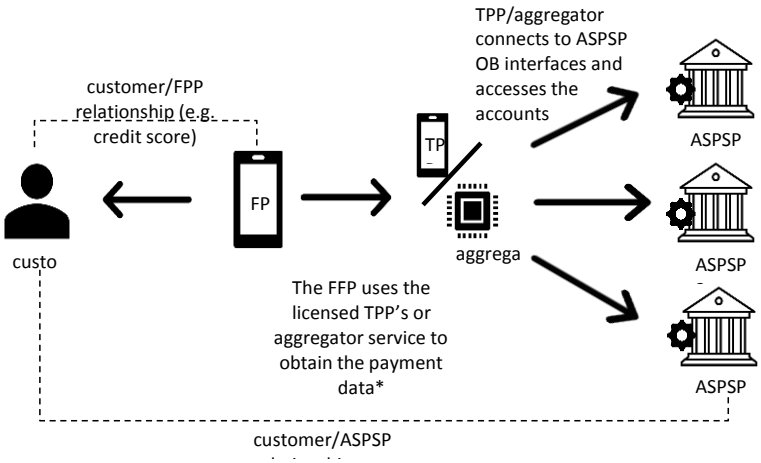


Figure 3 OB case with TPP/aggregator and unlicensed Fourth Party Provider



* The unlicensed FPP does not obtain access to the accounts. The customer is notified of the involvement of the TPP/aggregator.

OB interface, either dedicated (often API) or modified customer interface

It is important to note that these services already existed prior to PSD2, but that PSD2 brought these services (and consequently their providers) under scope and subjected them to authorisation, as it was identified that they could provide added value for consumers (ease of use and an alternative a credit card) and merchants (lower costs compared to credit cards, payment initiation confirmation, payment reconciliation). In line with this, it was decided to address both the legal uncertainty (no supervision, no regulation), the potential security risks in the payment chain and the lack of consumer protection. TPPs were usually accessing data via 'screen-scraping', without identifying themselves to the bank, which the banks often considered akin to hacking, therefore blocking the TPPs. By regulating the service, PSD2 gave the TPPs a legal basis to obtain access to a payment account, provided they received the consent of a payment service user to do so, and prevented banks from blocking the TPPs. By doing so, it also aimed to support the further development of PIS as an alternative to card payments.

3. HAS OB DELIVERED ON ITS INTENDED OBJECTIVES?

As detailed in the Evaluation (Annex 5), the market for Open Banking services has grown significantly, both in terms of number of TPPs, API calls, and users. This, however, does not mean that the current Open Banking regime laid out in PSD2 has been entirely successful, as evidenced in the limited awareness that consumers have of what Open Banking is, and in the relatively low degree of satisfaction with the regime expressed by both consumers, PSPs and TPPs in the public and targeted consultation (cf. Annex 5). This will be further examined here from the perspective of what putting OB in PSD2 tried to achieve: data protection/security, a legal framework for AIS and PIS (authorisation and supervision, but also rights and obligations), increasing competition, supporting innovation and lower costs to merchants for payments. Note that the indicators do not necessarily presume a causal relationship between the indicator and the regulation of Open Banking in PSD2, there is also too little data available for that.

3.1. The legal framework, data protection and security

In terms of data protection and security the PSD2 has ensured that TPPs must first be authorised and are subsequently supervised by a relevant national competent authority. This authorisation process requires, amongst others, a security policy document (PSD2 art. 5(1)j) with a *detailed risk assessment in relation to its payment services and a description of security control and mitigation measures taken to adequately protect payment service users against the risks identified, including fraud and illegal use of sensitive and personal data*. During authorisation a TPP's governance and risk management is also scrutinised for soundness and adequacy. Although it's difficult to say if TPPs active prior to PSD2 already had such measures in place (and if these were adequate), the TPPs active now, and able to provide services, are monitored and forced to actively work on security and data protection. Notably, the targeted consultation shows that PSD2 has contributed to safer data sharing:

65% of respondents *agree* that PSD2 ensures safe sharing of payments data, whereas 13% of respondents disagree (the others are neutral). Those that disagree (a mix of stakeholders, but no TPPs) do not provide further clarification[373].

Another important data protection and security topic that the PSD2 aimed to address, namely the unsecure sharing of personalised security credentials with (unauthorised) TPPs also received positive feedback: 78% of respondents find that the PSD2 protects the confidentiality and integrity of users personalised security credentials.[374] The previously observed unsecure situation of users directly sharing their log-in credentials with unauthorised TPPs who then used (and stored) those credentials to give them direct access to users payment accounts, has improved. Banks have put in place (dedicated) interfaces[375] that require TPPs to identify themselves to the banks and that would enable safer access to data and more secure processes around the use of personalised security credentials. TPPs themselves, especially those that were established post-PSD2 (like members of the Open Finance Association, OFA), indicate they prefer access to payment accounts via PSD2 APIs.[376]

3.2. Innovation and lower market barriers

The large increase in new TPPs can be correlated with the inclusion of Open Banking in PSD2. By mandating banks to provide access to data and legitimising the AISP and PISP-business models the barriers to access this market have been lowered. Where the PSD2 IA of 2013 focused almost solely on the opportunities PISPs could offer merchants, i.e. lower costs for payment transactions, the large number of AISPs is indicative of the opportunities this service can offer. AIS providers offer (new) services like (personal) financial management tools allowing for better spending, budgeting, and saving, but also to support loan applications. Especially PISPs also see opportunities for Open Banking in combination with Instant Payments.

However, some stakeholders (mostly the incumbents, pre-PSD2 TPPs) note that competition and innovation actually have not improved that much, notably where OB was already present before PSD2 (Nordics or Germany). Two reasons are mentioned most frequently by stakeholders through bilateral meetings, position papers, feedback to consultations and EBA Q&As:

---

[373] Except for BEUC, whose explanation (question 33b) covers a past data sharing concern (of over sharing) they had concerning PISPs access to account balance and outstanding (pipeline) payments, which would no longer be an issue with instant payments.

[374] Targeted consultation on PSD2, question 41.4: *The security measures introduced by PSD2 adequately protect the confidentiality and integrity of payment service users' personalised security credentials*

[375] Either interfaces that allow for direct customer interface connectivity (still requiring an exchange of eIDAS certificates, but thereafter screen-scraping) or dedicated PSD2 APIs (also requiring eIDAS certificates, but scoping the access to sec PSD2-accounts and information)

[376] OFA position paper on PSD2 – Open Finance Association

- Fragmented and sometimes non-compliant and low-quality technical implementation of access to accounts (APIs);
- Access to accounts has to be provided for free by banks to TPPs[377] while requiring significant investments from banks.

With regard to the first point above many TPPs say that even though the costs for API implementation were high to them, APIs (requirements) are implemented differently and don't always work, some data fields necessary to provide TPP services are not (always) provided and there is a high reliance on technical service providers due to API fragmentation. They criticise what they perceive to be regulators' and EBA's slow response to Q&As and provision of guidance and how PSD2 has been enforced, or rather, not enforced enough. Some non-TPPs made similar observations[378].

With regard to the second point: banks mostly complain about the costs of complying with PSD2 and allegedly being forced to fully bear those costs. The PSD2 does not allow for contractual obligations between banks and TPPs, so TPPs do not pay anything to the banks to access the payment accounts.

Reliable and verifiable evidence on the money spent by banks on facilitating access to accounts is limited: the VVA/CEPS study had to make a lot of assumptions and made a rough estimate of € 2.2 bln in total (one-off costs), using rather broad assumptions such as *"~40,400 person-days*" for banking groups and networks and "*1180 person-days per institution*" for smaller institutions, based on extremely limited stakeholder input. The stakeholder input however largely came from the institutions themselves, who often turn out to be unable to provide more specific figures solely on the implementation of access to accounts, or to distinguish IT-costs specifically related to PSD2 to those not related to PSD2. This is also visible in the feedback to our targeted consultation, where some respondents provided general figures such as "*double-digit million euro per institution"* (ESBG), or "*the overall one-off implementation costs were (far) in excess of 100M €*." (ING), with very few stakeholders providing more precise (but varying) figures: Credit Agricole reports €21ml and an association of Finnish banks reports "*3 to 8 million Euros (or higher*)".

In theory, various reasons might explain the differences: a bank's legacy infrastructures, which might be a factor for larger banking groups, a bank's IT capabilities and the quality of their financial reporting, to name a few. Banks furthermore stress that sometimes their APIs are not being used by TPPs, especially those servicing corporate payment accounts. The most frequent suggestion from banks is to amend the PSD2 to allow for remuneration or compensation for the facilitation of access to data (i.e. allowing for contractual obligations).

---

[377] PSD2, article 64(5) and 65(4): "*no contractual obligation*"

[378] Targeted consultation on PSD2, question 33.b: based on responses from Yapily, The Payments Association EU, Mastercard, BBVA, Tink AB, SOPRA STERIA, ETTPA, VIVA Payments. The EBA Call for Advice also observed the enforcement of PSD2 was not very effective and provides suggestions on how to improve this (EBA Call for Advice, Section 9 – Enforcement of PSD2)

This suggestion might also influence a bank's motivation to report high costs for the implementation of access to accounts. One could furthermore surmise that if the costs were truly very high, banks would have recouped these costs elsewhere, for example by increasing payment account fees.

Besides, it is important to note that the banks' implementation of access to payment accounts via APIs, despite their initial reluctance to provide access to data, is another piece of evidence for innovation in this market[379]. Banks have begun to implement the API technology to further their own business too, e.g. to provide Open Banking services themselves, and for non-PSD2 purposes. Direct customer interfaces have become API-based, and some banks are offering *commercial* APIs against a fee, next to the free PSD2-APIs that provide PSD2 services. Another advantage of implementing the API technology beyond just PSD2 is that it provides banks with a means to rid themselves of costly legacy systems[380].

The PSD2 Impact Assessment of 2013 assumed that the implementation costs for TPP access would be limited, on the basis that the information TPPs would access was already being provided to existing card schemes[381]. Based on the feedback we have received and the fact that both TPPs and banks not only had to spend many resources on setting up access to accounts, but also had to spend many resources on problem solving, as different interfaces had been set up with varying features, available data and overall quality. Faced with this, (some) TPPs in (some) markets make use of alternative solutions, including API aggregators (see illustrations above in section 1) or by continuing to use the fallback interface[382], inducing fees and adaption costs, respectively. This goes against the common assumption that access to accounts was free for TPPs. It is likely that some of these costs could have been avoided if access to the data through the interfaces had been effective. The level of costs to banks of setting up interfaces cannot be ascertained on the basis of the evidence available, but different interfaces would prevent exploiting economies of scale and scope, and therefore result in higher average costs. The additional resources required for problem solving also impact the costs for banks.

The above two issues combined led to a situation where TPPs were not always able to provide their services to customers (leading to complaints and lower use) and had to spend a lot of time discussing with banks and pleading their cause with supervisors. According to banks, the fact that they had to bear all the costs without getting anything in return did not

---

[379] Feedback from Targeted consultation and also observed in the National PSD2 Evaluation from the Netherlands.

[380] According to the VVA/ CEPS study (Annex 10), ASPSPs have begun to make efficiency gains (on a recurring basis).

[381] IA PSD2 Annex 2013, p. 223.

[382] According to the VVA/ CEPS study (Annex 10), TPPs spent about 35 million EUR on problems linked to accessing APIs, and 140 million EUR on maintaining legacy systems due to APIs not working properly. The figures provided via the study and other sources (targeted consultation, bilateral interaction) on the setting up of PSD2 APIs are difficult to determine, but vary from 3 million to "double digit"-millions and "in excess of 100 mln EUR" reported by single institution. The study estimates a (one-off) 2.2 bn EUR for all ASPSPs.

motivate them to pro-actively ensure compliance, or to behave cooperatively. Some banks even claim that this provision leads to double costs for them, because if they were to implement an innovation in their own direct channels in scope of PSD2, they would have to implement this too in the dedicated PSD2-interface[383].

In spite of the various challenges identified, both TPPs and bank-stakeholders wish to continue with Open Banking activities. The majority finds that the regulation surrounding Open Banking should be *adjusted* with an aim to improve its implementation, application, and adoption. This is also supported by the respondents' overall assessments of Open Banking in the EU, some of whom also point out the importance of fine-tuning this first, *before* extending access to accounts to other domains[384].

3.3. Merchants' savings from using PIS instead of cards

The IA on PSD2 of 2013 estimated large potential costs savings for merchants if they were to make use of PISPs and account-to-account-payments, instead of the more costly card payments. The IA estimated that savings would range from a minimum of 863 million € to a maximum of 3 520 million[385].

To assess whether any of these potential cost savings were met we would need to know the amount or number of PIS payments of merchants, but data on the use of PISPs in the EU is scarce. We have one indicative figure coming from the UK, where there were about 6 mln PIS calls in June 2022, against 2.1 bn card payments in the same month (UK Finance, June 2022). This means PIS would still only make up 0.3% of the UK Retail payments per June 2022, although the research indicates the numbers of PIS payments are growing month on month. Given this low percentage, the estimated IA savings have not been realised yet. But one should not lose sight of the fact that PSD2 OB measures only came into force 3 years ago, it might therefore still be too early to conclude that this objective will never be met.

When replying to our consultation, merchants agreed that there are more options available to make payments than 5 years ago and they find PSD2's Open Banking regime successful ("somewhat agree")[386]. They also say the overall benefits of PSD2 ("*standardisation, innovation and competition*") outweigh the (implementation) costs, but do not go into further detail. When merchants discuss PSD2, the discussion often focuses on the implementation of SCA and less on the (potential benefits from) Open Banking. No figures were provided by merchants regarding (PSD2) benefits.

---

[383] Targeted consultation on PSD2, question 33b: EACB, EBF, Febelfin, Finance Finland, Banca Sella Holding and others.

[384] Targeted consultation on PSD2, question 36: *What is your overall assessment about open banking in the EU? Would you say that it should be further extended?* – No: ESBG, BNP Paribas, Société Générale.

[385] IA PSD2 2013, p. 64-65.

[386] Targeted consultation on PSD2, question 2, 33.a. Eurocommerce.

4. ASSESSMENT OF THE OPEN BANKING MARKET OF THE UK

The UK took a more regulatory invasive and standardised implementation of Open Banking compared to the EU[387], which has not only resulted in less fragmentation in terms of APIs, but also in a more advanced Open Banking market and a somewhat higher adoption rate of OB[388]. The UK's implementation of Open Banking is coordinated by the Open Banking Implementation Entity (OBIE), which also gathers and publishes data on the API calls made via the banks under OBIE's scope[389] via API performance Stats. OBIE also publishes an Open Banking Impact Report every six months[390].

In terms of TPPs the UK is an attractive market: there were 212 TPPs being regulated in the UK by end Q3 2022[391], where there were 110 by November 2019. Regarding API calls and adoption of Open Banking services by users there is central data available on the largest 9 UK-banks ("CMA9"). The UK has been seeing on average approximately 1 bn monthly successful API calls since March 2022 (AIS and PIS combined), of which 6.6 mln successful API payments (increasing month-on-month by approximately 10%). Less than 1% of API calls fail (0.68%)[392]. Still, the market share of PIS payments vs. card payments is very low (0.3%, see above).

Consumer sentiment towards Open Banking is rather positive in the UK. The OBIE investigated the experiences of the users of Open Banking services in their Impact Report of October 202 on the use of Open Banking and the benefits users are gaining from it. A survey among users of Open Banking services showed that 76% intend to continue to use the service and report the OB platforms are "*helping them keep to budgets, reduce unnecessary expenditure, shop around and minimise fees and charges*". 64% reported that the apps had increased their total level of savings and 22% that the OB app was their "*first ever adult savings account*". The June 2022 Impact Report includes the results from a study on the use of cloud accounting services by small businesses (AIS), which is also largely positive (45% of respondents use them, 87% want to continue this use and >75% find that the service improves their (financial) business activities).

---

[387] The implementation of Open Banking went differently in the UK than in Europe. In 2017 (Brexit already in the works) the Competition and Markets Authority (CMA) came out with their Retail Banking Market Investigation report which concluded that banks should better serve their retail customers and small businesses. The CMA then ordered the 9 largest banks of the UK, the CMA9 to set up the OBIE and forced them to work together to implement Open Banking in a standardised way. This has largely meant that the UK's PSD2 API market was more standardised than the EU, and the UK being more advanced in their development and adoption of Open Banking.

[388] Konsentus: Open Banking in Review: Trends and Progress (December, 2021) Link to article: Link.

[389] The 9 mandated institutions (referred to as the CMA9) are: Barclays plc, Lloyds Banking Group plc, Santander, Danske, HSBC, RBS, Bank of Ireland, Nationwide and AIBG - CMA 9 - Open Banking.

[390] Open Banking Implementation Entity (OBIE), The open banking Impact Report, June 2022.

[391] Konsentus - Q3 2022 Konsentus Third Party Provider Open Banking Tracker, Link to article: Link.

[392] OBIE performance statistics September 2022 (Link to stats) and Open Banking adoption in the UK (OBIE Open Banking Impact Report June 2022) (Link to report).

All in all, the data shows that specifically for AIS services (potentially in combination with PIS, like sweeping) those using the service, a growing number, are largely positive about the benefits they get from the services and intend to continue using these services. Consumers indicate they are in better control of their personal finances and increased their savings, whereas small business respond the services improve their overall business.

In terms of ASPSP and TPP experiences in implementing Open Banking, most TPPs active in the UK and the EU find that the more standardised implementation in the UK was better and led to fewer problems. However, many TPPs believe it is too late for the EU to start implementing one API standard now, preferring more harmonisation of existing standards, supported by the EU but driven by the industry. Furthermore moving to a standard now would also imply significant costs for TPPs [393].

[393] Targeted Consultation Q34: *EU legislation on payments should include a common API standard*, responses from Yapily and OFA. This is also the feedback generally received when discussing this topic bilaterally with these parties, or in PSMEG.

ANNEX 12: COHERENCE WITH OTHER COMMISSION ACTS AND INITIATIVES

To complement Chapter 7.3 of the main impact assessment report, below is a detailed account of the coherence of the initiative with the key items of EU legislation and ongoing Commission initiatives (other than Open Finance, which is treated entirely in Chapter 7.3):

- *General Data Protection Regulation*. GDPR applies directly to all of the payment services concerned by PSD, separately and independently of PSD. The European Data Protection Board (EDPB) issued Guidelines in 2020 on the interplay of the Second Payment Services Directive and the GDPR[394]; regarding two key aspects covered in the EDPB Guidelines, "explicit consent" and "special categories of personal data", clarifications on the interaction of PSD/future PSR and GDPR will be provided in the proposal, further information about which is available in Annex 7. The retained option for exchange of information between PSPs on fraud does not comprise an obligation on PSPs to share information and therefore does not constitute a legal basis for exchange of personal data in the meaning of GDPR.
- *Markets in Crypto Assets Regulation (MiCA).* The proposed Regulation on Markets in Crypto Assets, politically agreed by the co-legislators but not yet legally in force, divides crypto assets into three types for regulatory purposes: e-money tokens (EMTs), asset-referenced tokens (ARTs), and other crypto assets. Of these three categories, only EMTs are categorised as funds and therefore payment transactions made with EMTs fall within the scope of PSD2. However, given the very specific nature of EMTs as a type of crypto asset (use of Distributed Ledger Technology etc), a certain number of clarifications are necessary in PSD2 in order to ensure certainty about the application of certain requirements (such as SCA) to payments using EMTs. Annex 7 provides more details about these clarifications.
- *Digital Operational Resilience Act.* PSPs providing payment services in the meaning of PSD are within the scope of DORA, and its provisions apply directly to them. However, payment system infrastructure operators, which are not in the scope of PSD2 nor of the proposed revision (see annex 6), are not within the scope of DORA. DORA requires the PSD2 review to consider the inclusion of "operators of payment systems and entities involved in payment–processing activities" within the scope of PSD2, which would consequently allow their inclusion within the scope of DORA[395].

---

[394] EDPB Guidelines 06/2020. The European PSP sector expressed concerns about these Guidelines as potentially hindering the objectives of PSD2 in a joint public letter. See also the Evaluation Report in Annex 5, section 4.1.3.2.

[395] Article 58 of DORA says: "*In the context of the review of Directive 2015/2366, the Commission shall assess the need for increased cyber resilience of payment systems and payment–processing activities and the appropriateness of extending of the scope of this Regulation to operators of payment systems and entities involved in payment–processing activities. In light of this assessment, the Commission shall submit, as part of*

Annex 6 of the present impact assessment, which will form the basis for the review report referred to in article 108 of PSD2, summarises the outcome of the reflections of the Commission to date on this subject, and its conclusion that there are currently no grounds to extend the scope of PSD to cover payment systems and technical service providers (including payment processors mentioned in DORA), but that this matter must be kept under close review, with a view to possible future legislation on payment systems and payment processors, separate from PSD.

- *Settlement Finality Directive*. Here it should be noted, as indicated in the evaluation (Annex 5) that currently SFD and PSD2 are coherent but with the consequence of excluding PIs and EMIs from payment systems designated under SFD. In amending PSD2 and/or SFD, care must be taken not to introduce any incoherence. For this reason, for example, it would not be possible to delete article 35.1(a) of PSD2 in isolation; this article exempts SFD-designated payment systems from a general obligation on payment systems to have rules on access which are proportional objective and non-discriminatory and removing it while leaving SFD unchanged would have created a conflict of law. The proposed combined changes to PSD2 and SFD would retain coherence, but with the positive effect of allowing PIs and EMIs to participate in payment systems designated by Member States under SFD, with appropriate safeguards.
- *The European Accessibility Act (EAA)*[396] is relevant, inter alia, for SCA execution. It covers consumer banking services including payment services, containing accessibility requirements for banking services in its scope in its Annex I section III and Section IV. For example it includes requirements prescribing the accessibility of products used in the provision of services and, specifically for banking services (including payments), prescribing that identification methods, electronic signatures, security and payment services must be perceivable, operable, understandable and robust. It also requires for banking services that information is understandable. Although the EEA departed from the barriers faced by 'persons with disabilities"[397] and elderly people, its requirements facilitate access in general, including for persons without disabilities. From that perspective, the measures described in Annex 10 to improve the ability of persons with disabilities and other persons with related challenges to use SCA would be coherent with the EAA by requiring that

---

the review of the Directive 2015/2366, a report to the Council and the EP no later than … [6 months from the date of entry into force of this Regulation].
Based on this review report, and after consulting EBA, ESMA, EIOPA, ECB and the ESRB, the Commission may submit, where appropriate and as part of the legislative proposal that it may adopt pursuant to Article 108, second paragraph, of Directive (EU) 2015/2366, a proposal to ensure that all operators of payment systems and entities involved in payment–processing activities are subject to an appropriate oversight, while taking into account existing central bank oversight."

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

[397] 'Persons with disabilities' means persons who have long-term physical, mental, intellectual or sensory impairments which in interaction with various barriers may hinder their full and effective participation in society on an equal basis with others.

identification methods, electronic signatures, security and payment services must be perceivable, operable, understandable and robust.

- *Interchange Fee Regulation*. To foster the Internal Market and competition in EU card payments, Regulation (EU) 2015/751 on interchange fees for card-based payment transactions (IFR) harmonizes diverging laws and administrative decisions and addresses restrictive business rules and practices. The IFR introduced caps for hitherto high interchange fees for consumer debit and credit cards, therefore setting harmonized ceilings for interchange fees for consumer cards in the EEA. The IFR also introduces business rules and aims at removing barriers to the internal market, such as restrictions on cross-border acquiring or the prevention of choice of payment brand or payment application for consumers and merchants. The IFR is closely related to PSD2, as the card-specific provisions of PSD2[398] complement the IFR in promoting entry, including of pan-European card schemes or in preventing payees from requesting charges for the use of payment instruments for which the interchange fees are regulated in the IFR. The preferred options remain coherent with the IFR, promoting innovative payment services, while keeping the PSD2 rules on surcharging for card-based payments.
- *Directive on Anti-Money Laundering and Countering the Financing of Terrorism* (AMLD, Directive 2015/849 as amended)[399]. Payment fraud leads to illicit revenues for criminals which are often subsequently laundered. Any reduction in payment fraud, which should result from the present initiative, should lead to a reduction in the amount of laundered funds. Moreover, the proposed measure to provide a legal basis for PSPs to share fraud data, parallels the provision in AMLD (article 39) allowing, in certain circumstances, Obliged Entities under that Directive to share information about suspicions of money laundering or terrorism financing. Weaknesses in internal AML controls are among the acceptable reasons for a bank to refuse to provide an account for a payment institution.

In addition, coherence should be considered with ongoing Commission initiatives which have not yet become legislation in force:

- *Commission legislative proposal on instant payments (amending the SEPA Regulation)*. The SEPA Regulation lays down harmonised rules and technical parameters for credit transfers and direct debits in euro. On 26 October 2022, the Commission adopted a proposal for an amendment of the SEPA Regulation concerning instant payments in euro, with four pillars:

[398] For instance, article 62 governing charges levied by payees on payers in respect of card-based payment transactions or 65 PSD2 on the confirmation on the availability of funds upon the request of PSPs issuing card-based payment instruments.

[399] A proposal for an amendment of this Regulation, including enactment of certain parts in a Regulation, was proposed by the Commission on 20 July 2021. See this link.

- An obligation on credit institutions which offer non-instant credit transfers to also offer instant credit transfers[400];
- An obligation not to price instant payments higher than corresponding regular credit transfers;
- An obligation on PSPs offering instant credit transfers to offer PSUs a service of verification of concordance of the payee's name and IBAN number, as a safeguard against fraudulent or erroneous payments.
- Procedural obligations on PSPs offering instant payments as regards penalties screening, in order to prevent undue failure of IPs while not impacting negatively the effectiveness of penalties screening.

PSPs offering credit transfers and direct debits in the meaning of the SEPA regulation, including instant payments, remain fully in the scope of PSD. A noteworthy element of the present initiative is the generalisation to all credit transfers in all EU currencies of the requirement in the Commission proposal on IPs regarding name/IBAN verification; this does not affect the proposal on IPs. Furthermore, direct access of PIs and EMIs to all EU payment systems would allow the extension of the scope of the proposal on IPs to include them (in a future review).

- *Data Act*. The Commission proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act), once adopted and in force, will establish a horizontal framework to which Open Banking, a service based on consensual access to data, will have to fully adhere. Regarding compensation, article 9 lays down that "*any compensation agreed between a data holder and a data recipient for making data available shall be reasonable*" and where the data recipient is a micro enterprise or an SME, the compensation must not exceed costs. However, the Data Act allows different provisions in sectoral legislation, and the requirement for Open Banking baseline account data access to be provided for free is an example of this.
- *Digital euro* A specific legislative proposal addressing the digital euro will be adopted in 2023, in line with the 2023's Commission Work Programme. This legislative proposal will however not address the rights obligations of the parties to a digital euro payment transaction. To ensure such coverage by legislation and the level playing field with regard to the legal obligations applicable to payment transactions with cash, scriptural money and e-money as the main categories of funds, and transactions with digital euros, the definition of funds needs to be amended, to include the digital euro as an explicit category of funds.
- *Commission legislative proposal of 3 June 2021 for a European Digital Identity Wallet (EDIW)*. The objective of the proposal is to set out harmonised conditions for the establishment of a framework for EDIWs. EDIWS are electronic identification means in the form of personal digital wallets. In particular, the proposal is meant to

[400] PIs and EMIs are not subjected to this obligation because currently they lack direct access to payment systems such as TARGET2 and TIPS, which is essential to carrying out this service.

allow users to digitally identify and authenticate online across borders, access a wide range of public and private online and offline services, such as banking and financial services, including retail payments. Secure electronic identification and the provision of attestation of attributes should offer additional flexibility and solutions for the financial services sector to support the fulfilment of strong customer authentication in the field of payment services. The proposal does not set aside the PSD2 acquis on SCA and related exemptions, neither the existing SCA solutions. PSPs should, however, also support the use of the EDIW where SCA is mandatory and the use of the Wallet is requested by the user. Depending on how the negotiations on the EDIW between the co-legislators proceed, the SCA rules under PSD2 might have to further assessed in light of the concrete features and additional benefits brought by the EDIW, such as mutual authentication (verifying that both payer and payee are who they say they are) or removing the need to redirect to ASPSPs.

ANNEX 13: SME TEST

The EU definition of SMEs is contained in Recommendation 2003/361. The category of micro, small and medium-sized enterprises consists of enterprises which:

- employ fewer than 250 persons; and
- have either an annual turnover not exceeding EUR 50 million or a balance sheet total not exceeding EUR 43 million.

SMEs are impacted by this initiative in two capacities, as users of payment services (such as merchants or business users) and as PSPs, including payment fintechs (smaller PSPs, start-ups etc.). They are thus on both the supply and demand side of the payments market. See section 1.4 of Annex 3.

(1) Preliminary assessment of businesses likely to be affected	
a) SMEs as users of payment systems All SMEs must use payment systems in order to receive and make payment of invoices. All SMEs are therefore affected as users. b) SMEs as Payment Service Providers The majority of banks including local and regional banks[401], qualify as SMEs under the above definition, and a significant number, possibly a majority, of payment institutions and e-money institutions are also SMEs, particularly fintechs and Open Banking Third Party Providers.	

[401] See CEPS study on the non-financial reporting directive, pp42: "about 19% of the banks are large" and "micro companies account for about 30% of all EU banks". (Notable that this study uses a slightly different size definition, based on the Accounting Directive, but the scale of thresholds are nonetheless comparable.) This is mainly due to the large number of small regional and savings banks, which are nonetheless common only in a few specific Member States, but which inflate the EU average size share for SME banks. These banks however often cooperate under national umbrella organizations, and such cooperation often covers operational aspects, such as development and deployment of APIs, resulting in significant efficiencies.

One EU banking association pointed out in an email that "when it comes to banks, the SME definition provided in the EU Recommendation 2003/361 does not really suit as – for evident reasons - even a rather small bank can have a balance sheet total above 43 million euros for instance". The CEPS study points out (page 40) that "The bank turnover consists mostly of net revenues such as net interest, net commission and net investment income, while the turnover of other (listed) companies and insurance companies is often based on gross revenues such as gross premium income." Meeting one of the two criteria (above employment) is enough for a bank to be categorized as SME under EU Recommendation 2003/361 and it seems that the bank turnover one is easier to miss. In any case, this illustrates the uncertainty as regards the application of the EU size criteria to banks.

(2) Consultation with SMEs representatives	
a) SMEs as users of payment systems No SME associations responded to the consultations and no individual SMEs contributed to the consultations in the capacity as users of payment systems, with the exception of the EFA (see below), which stressed the importance of full price transparency, including currency conversion charges, on payments going to beneficiaries outside the EU (so-called "one leg out" operations). b) SMEs as Payment Service Providers In the public and targeted consultations detailed in Annex 2, respondents were not asked to indicate whether they were SMEs, but bilateral contacts with bodies representative of Payment Institutions, E-Money institutions, fintechs and Open Banking Third Party Providers have taken place. The following associations provided specific input with regard to their representativity of SMEs: • European Fintech Association (EFA). 52% of its 40 members are SMEs. EFA requests inter alia more flexible requirements for payment institutions, better access for non-bank PSPs to payment systems, measures to deal with de-risking by banks, improvements to the functioning of SCA, improvements to the functioning of Open Banking, more flexibility for merchants to surcharge, more harmonious implementation of PSD2 across Member States. • Open Finance Association (OFA). 63% of its members are SMEs, and it considers that its input can be considered as largely representative of SME positions. OFA in its response to the targeted consultation pointed out inter alia that in its view the distinction between payment institution and e-money institution is outdated, the need to improve enforcement, ensure effective access to bank accounts (article 36) and improve the functioning of Open Banking. • European Payment Institution Federation (EPIF): about 70% of members are SMEs if direct and indirect membership (via national associations) is taken into account. EPIF in its response to the targeted consultation stressed inter alia the need to modernise PSD2, harmonise enforcement, improve access to payment systems for PIs, and introduce flexibility	Annex 10 SCA: 2.1.1, 5.2.1, 6.1.a); Open banking: 2.1.2, 5.2.2, 6.2; implementation: 2.1.3, 5.2.3, 6.3; access to payment systems: 2.1.4, 5.2.4, 6.4; surcharging: Annex 7; PI and EMI alignment: Annex 8.

(for example with the application of SCA).	
(3) Measurement of the impact on SMEs	
c) SMEs as users of payment systems For the purposes of this impact assessment, on the side of users of payment systems, no distinction has been made between users who are individual consumers and users who are businesses, including SMEs. SMEs will benefit from the measures to combat fraud, in particular as regards invoice fraud, which targets business including SMEs, and the user rights measures detailed in Annex 10 will assist SME users. d) SMEs as Payment Service Providers Many non-bank PSPs are SMEs, and therefore will benefit from the selected options to promote a level playing field between banks and non-bank PSPs. Many Open Banking TPPs (AISPs and PISPs) are SMEs, and will benefit from the improvements to the functioning of Open Banking. The administrative simplifications generated by the bringing together of the legislative frameworks for Payment Institutions and E-Money Institutions will benefit a significant number of PIs and EMIs which are SMEs.	Section 5.2.1, p25 and section 6.1., p31 Annex 10, p174 Section 5.2.4, p31 Open Banking: sections 2.1.2, 5.2.2, 6.2 Annex 8, p167
4) Assess alternative options and mitigating measures	
a) SMEs as users of payment systems Regarding SMEs as users of payment systems, the rejected option 1d (full reversal of liability between PSUs and PSPs for fraudulent authorised transactions), would have been of interest, but it was rejected for the reasons explained in section 6.1.d), including moral hazard and uncertainty about whether it would genuinely reduce fraud or merely redistribute the consequences of fraud. b) SMEs as Payment Service Providers Banks which are SMEs may be unduly impacted in their profitability by the management of a payment account for a payment institution or e-money institution being particularly complex, therefore this is	Section 5.2.2, p28 and 6.2.a), p37 Section 5.2.4, option 4a)

envisaged as an acceptable reason for such a bank to reject a request by a non-bank PSP for opening an account.	
Smaller payment institutions may, according to PSD2, be subjected by a Member State to a lighter regime with lighter supervisory requirements provided that certain thresholds regarding executed payment transactions are respected (article 108(e) in conjunction with article 32 of PSD2). This provision will be maintained in the review, with only an update of the thresholds for inflation. Many such exempted payment institutions will be SMEs, although the thresholds do not correspond exactly to the definition of SMEs in Recommendation 2003/361.	Thresholds: Annex 2 (p71), Annex 5 (p171), Annex 7
Regarding Open Banking, Option 2a (requirement for a dedicated interface) includes a provision allowing that exemptions from the requirement to provide a dedicated interface could be considered for cases where it may be disproportionate to require the ASPSP to offer a dedicated interface. This can be of particular interest to ASPSPs which are SMEs, with a niche or specialised business, although the exemption will not be based on size alone.	See p29 & p39