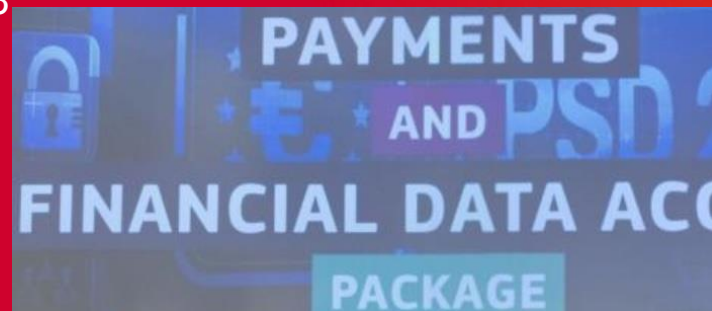


PSR

Payment Services Regulation

accompanying PSD3

EC 'PAYMENT' PACKAGE PROPOSED 28 JUNE 2023



Passion for payments

 **galitt**
a Sopra Steria company

We expected PSD3...

Why did we get also PSR?

— R = EU Regulation:



- └ Enforced with immediate effect EU-wide
- └ Therefore quickly (not like a Directive)



— PS = Payment Services

- └ Increases PSD2 objectives / targets
- └ Draws on its lengthy implementation and weaknesses / loopholes
- └ Merges together PSD2, its 'SCA-CSC' RTS and all related EBA 'Opinions'

→ More of PSD2... and more centralised

- └ Special EBA powers to suspend / ban risky products
- └ More, new RTS to come (6):  + new EBA Guidelines (3): 
- └ And... new special fines as a %age of turnover

PSR: what, how?

More ambitions, more legal instruments

— How to **get into / comply** with payment business?

(Authorisation / licensing, supervision by regulator)

→ **PSD3** (3rd Payment Services Directive)

— How to **perform** payment services?

(Rights & obligations of customers and their payment providers)

→ **PSR: Payment Services Regulation**

— How to offer **open** finance services **other** than payments?

→ **FIDA** (Financial Data Access Regulation)

REMINDER (no change)



- Placing / withdrawing cash
- Execution of payment transactions, incl. **if funds** covered by a **credit line** from own or 3rd-party PSP [*or prepaid*]
- Issuing of instruments
- Acquiring of transactions
- Money remittance
- Payment initiation services (PIS)
- Account information services (AIS)

+Includes EMD2 scope
= **prepaid payments**

Payment players newly impacted - or more

PSR directly addresses:

- Not only **licensed financial institutions (PSPs¹)**
but also:
- **Payment scheme operators**
 - └ Interbank SCA² routing servers (DS gateways)
- **Technical players :**
 - └ **ePSPs** (e-commerce payment acceptance providers) when not SCA-compliant
(= if they do not develop / maintain **SCA-enabling** solutions)
 - └ **Outsourced SCA providers** = providing and verifying SCA elements, e.g.:
 - xPay 'pass-through' wallet operators
 - ACS operators (ex.: SMS OTP-based challenges)
 - └ Other technical providers (e.g.: payment processors)

What's new in the draft PSR vs. PSD2?



- 01 Heavier fines
- 02 Authentication (SCA) extended
- 03 A better protected customer
- 04 Execution of payments improved
- 05 Streamlined open-banking
- 06 More transparency and client info
- 07 Fairer conditions of exercise

Turnover-based fines for most important PSR provisions

— Dedicated fines *[art. 97]*

- └ Up to **10 % of consolidated net turnover** (or up to € 5M for natural persons)
- └ **+** at least **twice the profits illegally gained**
- └ For breaches on:
 - Performance of **SCA** *[art. 85 à 87]* : by payer's PSP, by PISP / AISP, or by an outsourced provider/verifier of SCA element(s)
 - **Time limits to refund** / compensate payers for fraud:
 - D+1 and max. 10 days for fraud claims *[art. 56-2]*
 - 10 days for **failed IBAN check** *[art. 57-2]* and for **impersonation** fraud *[art. 59-2]*
 - **Secure open banking data access** (incl. use of customer interface by TPP in case of failure / emergency) *[Title III, Ch 3]*
 - **PI access to account** at a credit institution *[art. 32]*
 - **Info client on ATM withdrawals** (charges, interest rates and FX rates) *[art. 20-c-iii]*



— Daily penalty payments *[art. 98]*

- └ Up to **3% of same turnover** (or up to € 10k for natural persons)
- └ Until compliance, for max. **6 month** (for each decision)

— All sanctions decided by local regulator. Maximum amounts may be **raised locally** by Member States.



SCA: when and how to authenticate the payer?

Strong Customer Authentication: integrates & extends current EBA RTS & Opinions

- **SCA elements** do **not need** to be of **different categories** [art. 85-12]
- **'Inherence'** category to include payer's **behavioural data** [art. 83-2-a]
- **SCA by Account Information Service Providers, AISPs** [art. 86-3 & -4]:
 - └ AISP to refresh **themselves** SCA for account access every 180 days
 - └ ASPSP to apply SCA on **1st** AIS access only (for each AISP) **unless reasonable** grounds to suspect **fraud** (→ RBA)
- **MITs** outside of SCA scope **only if similar to direct debits**:
 - └ SCA on creation = **also** for mandate of **direct debit** when **concluded online**
 - └ if initiated "without any interaction or involvement" of the payer [art. 85-2]
 - └ when mandate-based: if no specific payer action needed (before payee triggers **user** instrument; *eg: card*) [art. 85-3]
- **MO-TO** payment to have security standards & checks, with a (simple) **payer authentication** [art. 85-7]
- **Dynamic link** (to payee amount & name) to apply on **POS** payments, when **user device** used for **SCA**
 - └ Ex: QR-code-initiated [art. 85-9]
- **Payer PSP to formalise SCA outsourcing** agreement if technical provider supplies & verifies SCA elements :
e.g.: ACS, xPay operators [art. 87]

A customer better protected (1/2)

— Extended refund right for the payer

The payer's PSP [art. 56]:



- └ **still** must refund as of D+1 of the payer's claim - And at the latest: **D+10** (vs. current D+30)
- └ unless it can prove payer fraud, to be **justified** to **payer** and notified to local regulator (ex: ACPR)

Now also for fraud cases:

- └ after **inoperant IBAN check** [art. 57]
- └ on MITs* without SCA, **depending on** designed **customer journey** [art. 60-2 et 85]
 - MIT without payer interaction or involvement prior to payee triggering payment:
 - **no SCA** required
 - → aligned on **direct debit** = '8 week' / '13 months' refund rules
 - MIT needing a **prior payer action** (*pay as you go, late charge...*):
 - **SCA required**
 - → refund if no SCA performed
- └ by **PSP impersonation** [art. 59]:
 - Applies to **consumers only**, if they report to the police (& their PSP) without delay
 - **Use cases: spoofing** (faked PSP phone number / SMS sender / mail address...)
 - Telcos mandated to cooperate (but no sanctions...)



A customer better protected (2/2)

- **Liability for failed SCA support by technical providers and payment scheme operators** [art. 58]
 - └ Among those involved = ePSPs, ACS providers, DS server operators (routing SCA requests), etc.
 - └ *NB: Payee PSP also liable if it “applies” SCA exemption [art.60-2] - but it has no operational role in SCA!*



- **Mandate for PSPs to monitor SCA risk and fraud risk** [art. 83]
 - └ Integrate and extends current “SCA” RTS
 - └ Analysis to include typical user location, time, device, spendings, online store...
 - └ Option to formalise an agreement to share fraud data via an IT exchange platform between PSP (e.g.: payee IBANs)
- **EBA intervention powers to suspend / block a specific payment service** [art. 104]
 - └ Special temporary powers in case of threat to users or markets



- **Information on new forms of fraud** [art. 84 + future Guidelines EBA]:
 - └ to **clients**: how to recognise/avoid and signal them (frequency = as need)
 - └ to **PSP staff** (annually at least)



- **Increased burden of proof on payer PSP to demonstrate correct functioning** [art. 55]
9 PSR
PSP fraud reporting: at least annually [Art. 82 + RTS-ITS]

Payment orders and execution improved

— IBAN check on (non-instant) credit transfers:

- └ Real-time check by payer PSP of **payee's IBAN and name** as **entered by payer** [art. 50]
- └ **Payer's PSP liable for fraud** if failure to provide the check [art. 57]
- └ *Reminder: IBAN check on **real-time** transfers **already** foreseen in draft **Inst. Payment Regulation** (IPR)*

— Limits to blocking of funds for amounts unknown in advance (cards) [art. 61]:

- └ **Real-time update** by merchant / payee to issuing PSP
- └ Proportionate amount

— Prohibition of surcharging [art. 28-3]:

- └ All payment methods in all EU currencies
- └ Except:
 - Commercial cards
 - Cash withdrawals
 - 3-party card schemes (excluding when issue/acquire through licensed partners or agents*)

Streamlined open-banking

— Client dashboard of TPP permissions *[art. 43]*

- └ Enables user to remove any AIS /PIS access in real-time
- └ Easy to find / use
- └ Similar to FIDA



— ASPSP obligation to have open-banking APIs (“dedicated interface”) *[art. 35]*

- └ Removal of mandatory fallback access (via user interface: Website/app connectors) *[art. 35]*
- └ But needs to be ready for contingency use by TPPs (upon regulator consent - & while waiting for it) *[38]*
- └ **NCA may exempt** from having a dedicated interface *[art. 39]*

— Same levels of **performance and functionality** than the ASPSP’s **direct** customer interface: more requirements *[art. 35 et 36]* and more reporting to EBA / EC *[Art. 48-7]*

— Little used “Confirmation of funds availability” (CoF) service **merged into PIS** (Payment Initiation Service) *[art. 36-5 a]*

More transparency and client information

— Estimating fund reception date and FX costs for transfers outside EEA [art. 13]

Mandatory real-time customer information, prior to validating order:

- └ When will the payee's PSP receive my funds?
- └ On currency conversion charges = estimated % mark-up on ECB €-FX rate (*aligned on intra-EEA rule*)

— Identifying payee (incl. commercial trade name) on account statements [art. 16 et 25]

- └ When confirming receipt of a payment order, and its execution
- └ Mentioning the payee's usual name known to the payer – *as per existing card schemes' requirement*

— Information on client charges for domestic ATM withdrawals [art. 20-c-ii]

- └ Charges whether ATM belongs to payer's PSP, its network, another contractually agreed network or an ISO*

— Info on Altern. Dispute Resolution (ADR) extended to single payments [art. 13-1-g + art. 90, 94 & 95]

— Termination for joint technical services: to be aligned with PSP own terms [art. 23]

- └ Like for the PSP's, termination of technical subcontractors supporting payment services must be **free** of charge **6 months** or later **after conclusion** of user framework-agreement.
- └ They must be **proportionate** if any.



Fairer conditions of exercise

— Equal access to payment systems *[art. 31]*

- └ **All systems'** access rules to be non-discriminatory, objective & proportionate
- └ With prior **risk assessment**
- └ Right of appeal of any refusal (notified in writing)

— **PI access to account at credit institutions** *[art. 32]*

- └ A condition for (applicant) Payment Institution (PIs) and their distributors and agents
- └ Refusal must be **notified** on serious grounds, e.g: illegal activity, risk for the credit institution



Annex: Focus on Open Banking

PSR: 10 takeaways for open banking

1



ASPSPs are mandated to provide dedicated interfaces (i.e. regulated APIs), unless an exemption is granted by the authorities

2



ASPSPs must provide permission dashboards where users can monitor, withdraw and review data access by TPPs

3



Parity with customer interface as main principle for dedicated interfaces from an SCA, functional and performance PoV

4



In addition to instruction on how to impose sanctions, the PSR provides 12 obstacles that must be removed from APIs (.../...)

5



No fallback interface, but TPPs may take contingency measures for non-performing dedicated interfaces

6



AISP enforces SCA to renew access after 180 days of access expires, but the ASPSP enforces the first time

7



ASPSP fraud reimbursements not limited to unauthorised transactions, but will also include APP scams

8



ASPSPs responsible to perform Name-IBAN matching, aka confirmation of payee (CoP), for manual credit transfers

9



SCA to permit two of the same factors and behavioral analytics as element of inherence

10



E-Money Directive (EMD) into the scope of the PSD text and treats e-money as one of the PSD services

Open banking in PSR: removing obstacles in regulated APIs

The ASPSP may not...

1. Prevent TPPs from using the PSU's credentials
2. Require PSUs to manually input their unique identifier (e.g.: IBAN) after being redirected
3. Check consent or permissions
4. Requiring additional registrations by TPPs to connect to the API
5. Require that TPPs pre-register their contact details for the permissions dashboard
6. Restrict PSUs to only initiate payments to a beneficiaries list
7. Restrict payments to or from domestic unique identifiers (e.g. IBAN) only
8. Require SCA more times when using TPP services than in the customer interface
9. Provide an API that does not support all SCA procedures available in the customer interface
10. Impose a 'redirection' or 'decoupled' approach where it creates unnecessary friction / adds additional steps
11. Impose 'redirection' to ASPSP's authentication as the sole method for SCA
12. Requiring 2 SCAs in a PIS-only journey, also when performing confirmation of funds, unless objective reason to do so.